

# Operating Manual

# VIP4G

**VIP4G LTE Ethernet Bridge/Serial Gateway**  
**Document: VIP4G Operating Manual.v1.1.pdf**

**August 2012**



150 Country Hills Landing NW  
Calgary, Alberta  
Canada T3K 5P3

Phone: (403) 248-0028  
Fax: (403) 248-2762  
[www.microhardcorp.com](http://www.microhardcorp.com)

## Important User Information

---

### Warranty

Microhard Systems Inc. warrants that each product will be free of defects in material and workmanship for a period of one (1) year for its products. The warranty commences on the date the product is shipped by Microhard Systems Inc. Microhard Systems Inc.'s sole liability and responsibility under this warranty is to repair or replace any product which is returned to it by the Buyer and which Microhard Systems Inc. determines does not conform to the warranty. Product returned to Microhard Systems Inc. for warranty service will be shipped to Microhard Systems Inc. at Buyer's expense and will be returned to Buyer at Microhard Systems Inc.'s expense. In no event shall Microhard Systems Inc. be responsible under this warranty for any defect which is caused by negligence, misuse or mistreatment of a product or for any unit which has been altered or modified in any way. The warranty of replacement shall terminate with the warranty of the product.

### Warranty Disclaims

Microhard Systems Inc. makes no warranties of any nature of kind, expressed or implied, with respect to the hardware, software, and/or products and hereby disclaims any and all such warranties, including but not limited to warranty of non-infringement, implied warranties of merchantability for a particular purpose, any interruption or loss of the hardware, software, and/or product, any delay in providing the hardware, software, and/or product or correcting any defect in the hardware, software, and/or product, or any other warranty. The Purchaser represents and warrants that Microhard Systems Inc. has not made any such warranties to the Purchaser or its agents MICROHARD SYSTEMS INC. EXPRESS WARRANTY TO BUYER CONSTITUTES MICROHARD SYSTEMS INC. SOLE LIABILITY AND THE BUYER'S SOLE REMEDIES. EXCEPT AS THUS PROVIDED, MICROHARD SYSTEMS INC. DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PROMISE.

**MICROHARD SYSTEMS INC. PRODUCTS ARE NOT DESIGNED OR INTENDED TO BE USED IN ANY LIFE SUPPORT RELATED DEVICE OR SYSTEM RELATED FUNCTIONS NOR AS PART OF ANY OTHER CRITICAL SYSTEM AND ARE GRANTED NO FUNCTIONAL WARRANTY.**

### Indemnification

The Purchaser shall indemnify Microhard Systems Inc. and its respective directors, officers, employees, successors and assigns including any subsidiaries, related corporations, or affiliates, shall be released and discharged from any and all manner of action, causes of action, liability, losses, damages, suits, dues, sums of money, expenses (including legal fees), general damages, special damages, including without limitation, claims for personal injuries, death or property damage related to the products sold hereunder, costs and demands of every and any kind and nature whatsoever at law.

IN NO EVENT WILL MICROHARD SYSTEMS INC. BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, BUSINESS INTERRUPTION, CATASTROPHIC, PUNITIVE OR OTHER DAMAGES WHICH MAY BE CLAIMED TO ARISE IN CONNECTION WITH THE HARDWARE, REGARDLESS OF THE LEGAL THEORY BEHIND SUCH CLAIMS, WHETHER IN TORT, CONTRACT OR UNDER ANY APPLICABLE STATUTORY OR REGULATORY LAWS, RULES, REGULATIONS, EXECUTIVE OR ADMINISTRATIVE ORDERS OR DECLARATIONS OR OTHERWISE, EVEN IF MICROHARD SYSTEMS INC. HAS BEEN ADVISED OR OTHERWISE HAS KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND TAKES NO ACTION TO PREVENT OR MINIMIZE SUCH DAMAGES. IN THE EVENT THAT REGARDLESS OF THE WARRANTY DISCLAIMERS AND HOLD HARMLESS PROVISIONS INCLUDED ABOVE MICROHARD SYSTEMS INC. IS SOMEHOW HELD LIABLE OR RESPONSIBLE FOR ANY DAMAGE OR INJURY, MICROHARD SYSTEMS INC.'S LIABILITY FOR ANY DAMAGES SHALL NOT EXCEED THE PROFIT REALIZED BY MICROHARD SYSTEMS INC. ON THE SALE OR PROVISION OF THE HARDWARE TO THE CUSTOMER.

### Proprietary Rights

The Buyer hereby acknowledges that Microhard Systems Inc. has a proprietary interest and intellectual property rights in the Hardware, Software and/or Products. The Purchaser shall not (i) remove any copyright, trade secret, trademark or other evidence of Microhard Systems Inc.'s ownership or proprietary interest or confidentiality other proprietary notices contained on, or in, the Hardware, Software or Products, (ii) reproduce or modify any Hardware, Software or Products or make any copies thereof, (iii) reverse assemble, reverse engineer or decompile any Software or copy thereof in whole or in part, (iv) sell, transfer or otherwise make available to others the Hardware, Software, or Products or documentation thereof or any copy thereof, except in accordance with this Agreement.

## Important User Information (continued)

---

### About This Manual

It is assumed that users of the products described herein have either system integration or design experience, as well as an understanding of the fundamentals of radio communications.

Throughout this manual you will encounter not only illustrations (that further elaborate on the accompanying text), but also several symbols which you should be attentive to:

**Caution or Warning**

Usually advises against some action which could result in undesired or detrimental consequences.

**Point to Remember**

Highlights a key feature, point, or step which is noteworthy. Keeping these in mind will simplify or enhance device usage.

**Tip**

An idea or suggestion to improve efficiency or enhance usefulness.

**Information**

Information regarding a particular technology or concept.

## Important User Information (continued)

---

### Regulatory Requirements



**WARNING**

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23cm or greater for the VIP2400 utilizing a 3dBi antenna, or 3.5m or greater for the VIP5800 utilizing a 34dBi antenna, should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna being used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.



**WARNING**

This device can only be used with Antennas approved for this device. Please contact Microhard Systems Inc. if you need more information or would like to order an antenna.



**WARNING**

**MAXIMUM EIRP**

FCC Regulations allow up to 36dBm Effective Isotropic Radiated Power (EIRP). Therefore, the sum of the transmitted power (in dBm and not to exceed +30dBm)), the cabling loss, and omnidirectional antenna gain cannot exceed 36dBm.

## CSA Class 1 Division 2 Option

---

### **CSA Class 1 Division 2 is Available Only on Specifically Marked Units**

If marked this for Class 1 Division 2 – then this product is available for use in Class 1, Division 2, in the indicated Groups on the product.

In such a case the following must be met:

The transceiver is not acceptable as a stand-alone unit for use in hazardous locations. The transceiver must be mounted within a separate enclosure, which is suitable for the intended application. Mounting the units within an approved enclosure that is certified for hazardous locations, or is installed within guidelines in accordance with CSA rules and local electrical and fire code, will ensure a safe and compliant installation.

Do not connect or disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

Installation, operation and maintenance of the transceiver should be in accordance with the transceiver's installation manual, and the National Electrical Code.

Tampering or replacement with non-factory components may adversely affect the safe use of the transceiver in hazardous locations, and may void the approval.

The wall adapters supplied with your transceivers are NOT Class 1 Division 2 approved, and therefore, power must be supplied to the units using the screw-type or locking type connectors supplied from Microhard Systems Inc. and a Class 1 Division 2 power source within your panel.

If you are unsure as to the specific wiring and installation guidelines for Class 1 Division 2 codes, contact CSA International.

## Revision History

---

Revision	Description	Initials	Date
1.0	Initial Release	PEH	June 2012
1.1	Updated Screen shots, Firewall settings, added VPN settings	PEH	August 2012

## Table of Contents

---

<b>1.0 Overview .....</b>	<b>10</b>
1.1 Performance Features .....	10
1.2 Specifications .....	11
<b>2.0 QUICK START .....</b>	<b>13</b>
2.1 Installing the SIM Card .....	13
2.2 Getting Started with Cellular .....	13
2.3 Getting Started with WiFi .....	17
2.3.1 Setting up WiFi .....	17
2.3.1 Connecting to WiFi .....	18
<b>3.0 Hardware Features .....</b>	<b>20</b>
3.1 VIP4G .....	20
3.1.1 VIP4G Mechanical Drawings .....	21
3.1.2 VIP4G Connections .....	22
3.1.2.1 Front .....	22
3.1.2.2 Rear .....	23
3.1.3 VIP4G Indicators .....	25
<b>4.0 Configuration.....</b>	<b>26</b>
<b>4.0 Web User Interface.....</b>	<b>26</b>
4.0.1 Logon Window.....	27
<b>4.1 System.....</b>	<b>28</b>
4.1.1 Summary .....	28
4.1.2 Settings.....	29
Host Name.....	29
Date/Time .....	30
NTP Server Settings.....	31
HTTP Port Settings.....	31
HTTPS Port Settings .....	31
4.1.3 Access Control .....	32
Password Change .....	32
Users .....	33
4.1.4 Services.....	34
RSSI LED's.....	34
SSH .....	34
Telnet.....	34
4.1.5 Maintenance .....	35
Version Information .....	35
Firmware Upgrade.....	35
Reset to Default.....	36
Backup & Restore Configurations .....	36
4.1.6 Reboot.....	37
4.1.7 Logout.....	38
<b>4.2 Network .....</b>	<b>39</b>
4.2.1 Status .....	39
4.2.2 Networks.....	40
LAN Configuration .....	41
WAN Configuration.....	42
DNS Configuration.....	42

## Table of Contents

4.2.3	DHCP .....	43
	LAN DHCP .....	43
	Static IP Addresses (For DHCP) .....	44
	Active DHCP Leases .....	44
4.2.4	VLAN .....	45
4.2.5	Routes .....	47
	Static Route Configuration .....	47
	Dynamic Route Configuration .....	48
4.2.6	GRE .....	49
4.2.7	SNMP .....	51
4.2.8	sdpServer .....	54
	Discovery Server Status .....	54
<b>4.3</b>	<b>Carrier .....</b>	<b>55</b>
4.3.1	Status .....	55
4.3.2	Settings .....	56
	APN (Access Point Name) .....	56
4.3.3	Keepalive .....	59
4.3.4	Traffic Watchdog .....	60
4.3.5	Dynamic DNS .....	61
<b>4.4</b>	<b>Wireless .....</b>	<b>62</b>
4.4.1	Status .....	62
	General Status .....	62
	Traffic Status .....	62
4.4.2	Radio1 .....	63
	Radio Phy Configuration .....	63
	802.11 Mode .....	63
	Channel BandWidth .....	63
	Channel Frequency .....	64
	Radio Virtual Interface .....	65
	Operating Mode .....	66
	TX Rate .....	66
	TX Power .....	67
	SSID .....	67
	Encryption Type .....	68
<b>4.4</b>	<b>Comport .....</b>	<b>69</b>
4.4.1	Status .....	69
4.4.2	Settings .....	70
	Data Baud Rate .....	71
	IP Protocol Config .....	74
	TCP Client .....	74
	TCP Server .....	74
	TCP Client/Server .....	75
	UDP Point-to-Point .....	75
	UDP Point-to-Multipoint (P) .....	75
	UDP Point-to-Multipoint (MP) .....	76
	UDP Multipoint-to-Multipoint .....	76
	SMTP Client .....	77
<b>4.5</b>	<b>I/O .....</b>	<b>78</b>
4.5.1	Inputs .....	78
4.5.2	Outputs .....	79



## Table of Contents

---

<b>4.6 Firewall .....</b>	<b>80</b>
4.6.1 Status .....	80
4.6.2 General .....	81
4.6.3 Rules .....	83
4.6.4 Port Forwarding .....	85
DMZ .....	85
4.6.5 MAC-IP List .....	87
MAC List Configuration .....	87
IP List Configuration .....	88
<b>4.7 Multicast .....</b>	<b>89</b>
Multicast Configuration .....	89
<b>4.8 QoS .....</b>	<b>91</b>
4.8.1 Status .....	91
4.8.2 Class .....	92
4.8.3 Local .....	93
4.8.4 Interface .....	95
<b>4.9 VPN .....</b>	<b>96</b>
4.9.1 Summary .....	96
4.9.2 Gateway to Gateway .....	97
4.9.3 Client to Gateway (L2TP Client) .....	101
4.9.4 L2TP Server .....	103
4.9.5 VPN Client Access .....	104
<b>4.9 Tools .....</b>	<b>105</b>
4.9.1 Discovery .....	105
4.9.2 Site Survey .....	106
Wireless Survey .....	106
4.9.3 Ping .....	107
4.9.4 TraceRoute .....	108
4.9.5 Network Traffic .....	109
<b>Appendices .....</b>	<b>110</b>
Appendix A: Serial Interface .....	110
Appendix C: Firmware Recovery .....	111

## 1.0 Overview

---

The VIP4G is a high-performance 4G LTE Cellular Ethernet & Serial Gateway with 802.11 a/b/g/n WiFi capability, 4 Gigabit Ethernet Ports, 4x Digital I/O, and a fully complimented RS232/485/422 serial port.

The VIP4G utilizes the cellular infrastructure to provide network access to wired and wireless devices anywhere cellular coverage is supported by a cellular carrier. The VIP4G supports up to 100Mbps when connected to a LTE enabled carrier, or global fallback to 3G/Edge networks for areas without 4G LTE.

Providing reliable wireless Ethernet bridge functionality as well gateway service for most equipment types which employ an RS232, RS422, or RS485 interface, the VIP4G can be used in a limitless number and types of applications such as:

- High-speed backbone
- IP video surveillance
- Voice over IP (VoIP)
- Ethernet wireless extension
- WiFi Hotspot
- Legacy network/device migration
- SCADA (PLC's, Modbus, Hart)
- Facilitating internetwork wireless communications

### 1.1 Performance Features

Key performance features of the VIP4G include:

- Fast 4G LTE Link to Wireless Carrier
- Up to 100Mbps Downlink / 50 Mbps Uplink
- Fast Data Rates to 802.11a/b/g/n WiFi Devices
- Digital I/O - 4 Inputs, 4 Outputs
- DMZ and Port Forwarding
- 4 - 10/100/1000 Ethernet Ports (WAN/LAN)
- Integrated GPS (TCP Server/UDP Reporting)
- User interface via local console, telnet, web browser
- communicates with virtually all PLCs, RTUs, and serial devices through either RS232, RS422, or RS485 interface
- Local & remote wireless firmware upgradable
- User configurable Firewall with IP/MAC ACL
- IP/Sec secure VPN and GRE Tunneling

## 1.0 Overview

---

### 1.2 Specifications

For detailed specifications, please see the specification sheets available on the Microhard website @ <http://www.microhardcorp.com> for your specific model.

#### Electrical/General

##### Cellular:

**Supported Bands:** 4G LTE AWS 700 MHz (with MIMO)  
Global Fallback to:  
HSPA+/UMTS 850/AWS/1900/2100 MHz  
GPRS 850/900/1800/1900 MHz

**Data Features:** 4G LTE  
Up to 100 Mbps downlink  
Up to 50 Mbps uplink

**SIM Card:** 1.8 / 3.0 V

##### WiFi:

**Frequency:** 2.4 GHz / 5.8 GHz

**Spread Method:** OFDM/QPSK/16QAM/64QAM

**Data Rates:** 802.11a/b/g/n

**TX Power:** Adjustable / Up to 30dBm

**Data Encryption:** WEP, WPA(PSK), WPA2(PSK), WPA+WPA2 (PSK)  
(Subject to Export Restrictions)

##### General:

**Input Voltage:** 7 - 30 VDC

**Serial Baud Rate:** 300bps to 921kbps

**Ethernet:** 10/100/1000 BaseT, Auto - MDI/X, IEEE 802.3

**Network Protocols:** TCP, UDP, TCP/IP, TFTP, ARP, ICMP, DHCP, HTTP, HTTPS\*, SSH\*, SNMP, FTP, DNS, Serial over IP

**Operating Modes:** Access Point, Client/Station, Repeater, Mesh Point

**Management:** Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade

**Diagnostics:** Status LED's, RSSI, Ec/No, Temperature, Remote Diagnostics, Watchdog, UDP Reporting

**Digital I/O:** 4 Inputs / 4 Outputs

## 1.0 Overview

---

### 1.2 Specifications (Continued)

#### Environmental

**Operation Temperature:** -40°F(-40°C) to 185°F(85°C)

**Humidity:** 5% to 95% non-condensing

#### Mechanical

**Dimensions:**

5.65" (145mm) X 3.72" (95mm) X 1.20" (30mm)

**Weight:**

Approx. 405 grams

**Connectors:**

**Antenna:** Wi-Fi: 2x SMA Female  
Cellular: 2x SMA Female (Main, DIV)  
GPS: 1x SMA Female

**Data:** RS232 Data: DE-9 Female  
RS485: SMT: 6-Pin Micro MATE-N-LOK AMP 3-794618-6  
Mating Connector: 6-Pin Micro MATE-N-LOK AMP 794617-6  
Ethernet: 4x RJ-45

**PWR, Misc:** Power: SMT: 4-Pin Micro MATE-N-LOK AMP 3-794618-4  
Mating Connector: 4-Pin Micro MATE-N-LOK AMP 794617-4

**Misc:** Digital I/O: SMT: 10-Pin Micro MATE-N-LOK AMP 4-794618-0  
Mating Connector: 10-Pin Micro MATE-N-LOK AMP 1-794617-0

## 2.0 Quick Start

This QUICK START guide will walk you through the setup and process required to access the WebUI configuration window and to establish a basic wireless connection to your carrier.

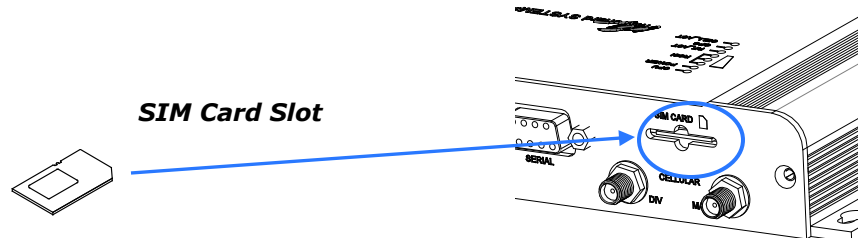
Note that the units arrive from the factory with the Local Network setting configured as 'Static' (IP Address 192.168.168.1, Subnet Mask 255.255.255.0, and Gateway 192.168.168.1), in DHCP server mode. (This is for the LAN Ethernet Adapter on the back of the VIP4G unit.)

### 2.1 Installing the SIM Card



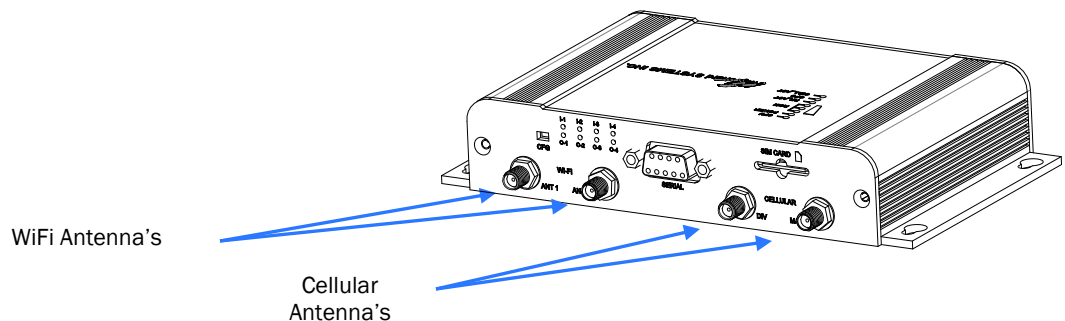
To reset to factory defaults, press and hold the CFG button for 8 seconds with the VIP4G powered up. The LED's will flash quickly and the IP4G will reboot with factory defaults.

- ✓ Before the IPn3G can be used on a cellular network a valid **SIM Card** for your Wireless Carrier must be installed. Insert the SIM Card into the slot as shown below.



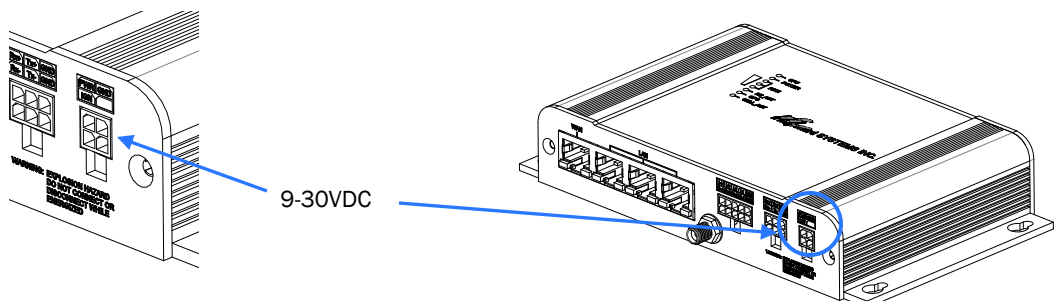
### 2.2 Getting Started with Cellular

- ✓ Connect the Antenna's to the applicable **ANTENNA** jack's of the IPn3G.



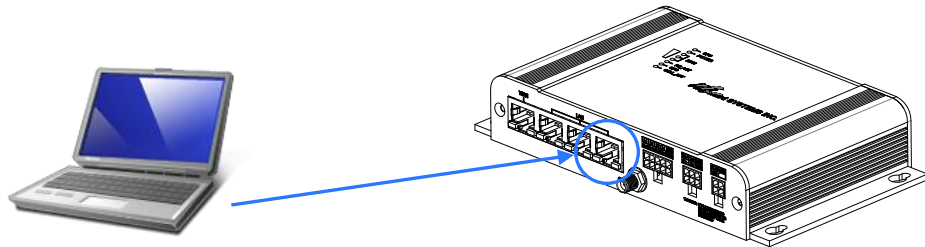
Use the MHS-supplied power adapter or an equivalent power source.

- ✓ Connect the power connector to the power adapter and apply power to the unit, once the blue CPU LED is on solid, proceed to the next step.



## 2.0 Quick Start

- ✓ Connect A PC configured for DHCP directly to one of the LAN **ETHERNET** ports of the VIP4G, using an Ethernet Cable. If the PC is configured for DHCP it will acquire a IP Address from the VIP4G.



- ✓ Open a Browser Window and enter the IP address 192.168.168.1 into the address bar.



The factory default network settings:

**IP: 192.168.168.1**  
**Subnet: 255.255.255.0**  
**Gateway: 192.168.168.1**



192.168.168.1

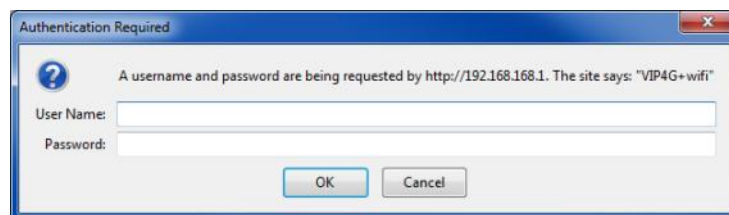
- ✓ The IPn3G will then ask for a Username and Password. Enter the factory defaults listed below.



The factory default login:

**User name: admin**  
**Subnet: admin**


It is always a good idea to change the default admin login for future security.





## 2.0 Quick Start

- ✓ Once successfully logged in, the System Summary page will be displayed.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	Tools
Summary	Settings	Access Control	Services	Maintenance	Reboot	Logout			
System Information									
System Information					Carrier Status				
System:					Module Status		Enabled		
Host Name		VIP4G+wifi			Current APN		Unknown		
System date		1970-01-01			Activity Status		Disconnected		
System time		00:00:49			Network		Bell		
System uptime		0 min			Home/Roaming		Home		
Version:					Current Technology		HSUPA		
Product Name		VIP4G+wifi			Core Temperature(°C)		28		
Firmware Version		VIP 2.0			IMEI		012773002004297		
Hardware Type		v2.0.0			SIM Number (ICCID)		89302610202061722946		
Build Version		v1.1.2 build 1076			Phone Number		14034635915		
Built date		2012-05-10			RSSI (dBm)		-54 dBm		
Built time		16:10:44			Connection Duration		0		


- ✓ As seen above under Carrier Status, the SIM card is installed, but an APN has not been specified. Click on the Carrier > Carrier TAB and enter the APN supplied by your carrier in the APN field. Some carriers may also require a Username and Password.

System				Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	Tools					
Status				Carrier	Keepalive	Traffic Watchdog	Dynamic_DNS										
Carrier Configuration																	
Configuration																	
Carrier status				Enable ▾													
APN				<input type="text"/>													
SIM Pin				<input type="text"/>													
Technologies Type				ALL ▾													
Technologies Mode				AUTO ▾													
Data Call Parameters				<input type="text"/>													
Primary DNS Address				<input type="text"/>													
Secondary DNS Address				<input type="text"/>													
Primary NetBIOS Name Server				<input type="text"/>													
Secondary NetBIOS Name Server				<input type="text"/>													
Address				<input type="text"/>													
IP Address				<input type="text"/>													
Authentication				Device decide ▾													
User Name				<input type="text"/>													
Password				<input type="text"/>													

- ✓ Once the APN and any other required information is entered to connect to your carrier, click on "Submit". Return to the System > Summary tab.

## 2.0 Quick Start

- ✓ On the Carrier > Status Tab, verify that a WAN IP Address has been assigned by your carrier. The Activity Status should also show "Connected".

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
Status	Settings	Keepalive	Traffic Watchdog	Dynamic DNS						
Carrier Status										
Carrier Status										
Current APN	Itemobile.apn		Core Temperature(°C)	51						
Activity Status	Connected		IMEI	012773002003661						
Network	ROGERS		SIM PIN	READY						
Home/Roaming	Home		SIM Number (ICCID)	89302720403007563694						
Service Mode	Automatic		Phone Number	+14035619334						
Service State	WCDMA CS and PS		RSSI (dBm)	-63 						
Cell ID	58003		RSRP (dBm)	N/A						
LAC	63333		RSRQ (dBm)	N/A						
Current Technology	HSPA+		Connection Duration	12 min 2 sec						
Available Technology	UMTS, HSDPA, HSUPA, HSPA+		WAN IP Address	25.88.118.79						
			DNS Server 1	64.71.255.198						
			DNS Server 2	64.71.255.253						
Recieved Packet Statistics					Transmitted Packet Statistics					
Recieve bytes	9.465MB		Transmit bytes	1.834MB						
Recieve packets	7988		Transmit packets	6311						
Recieve errors	0		Transmit errors	0						
Drop packets	0		Drop packets	0						
<div>Stop Refreshing</div> Interval: 20 (in seconds)										

- ✓ Congratulations! Your VIP4G is successfully connected to your Cellular Carrier. The next section gives a overview on enabling and setting up the WiFi Wireless features of the modem giving 802.11 devices network access.



## 2.0 Quick Start

### 2.3 Getting Started with WiFi

This **Quick Start** section walks users through setting up a basic WiFi AP (Access Point). For additional settings and configuration considerations, refer to the appropriate sections in the manual. This walkthrough assumes all settings are in the factory default state.



#### 2.3.1 Setting up WiFi

- ✓ Use **Section 2.2** *Getting Started with Cellular* to connect, power up and log in and configure the Carrier in a VIP4G.
- ✓ Click on the Wireless > Radio1 Tab to setup the WiFi portion of the VIP4G.

System Network Carrier **Wireless** Comport I/O Fire

Status **Radio1**

**Wireless Configuration**

**Radio1 Phy Configuration**

Radio ☒ On ☐ Off

Mode 802.11NG - High Throughput on 2.4GHz

High Throughput Mode HT20

Advanced Capabilities ☐ Show

Channel-Frequency 11 - 2.462 GHz

Wireless Distance 10000 (m)

RTS Thr (256~2346) ☒ OFF

Fragment Thr (256~2346) ☒ OFF

**Radio1 Virtual Interface**

Network LAN

Mode Access Point

TX bitrate Auto

Tx Power 17 dbm

WDS ☒ On ☐ Off

ESSID Broadcast ☒ On ☐ Off

SSID MyNetwork

Encryption Type WPA2 (PSK)

WPA PSK MyPassword

Show password ☒

In **Radio1 Phy Configuration**, ensure the mode is set for 802.11NG.

In the **Radio1 Virtual Interface**, ensure that the Mode is set for Access Point.

Enter a name for the Wireless Network under **SSID**. This example uses MyNetwork

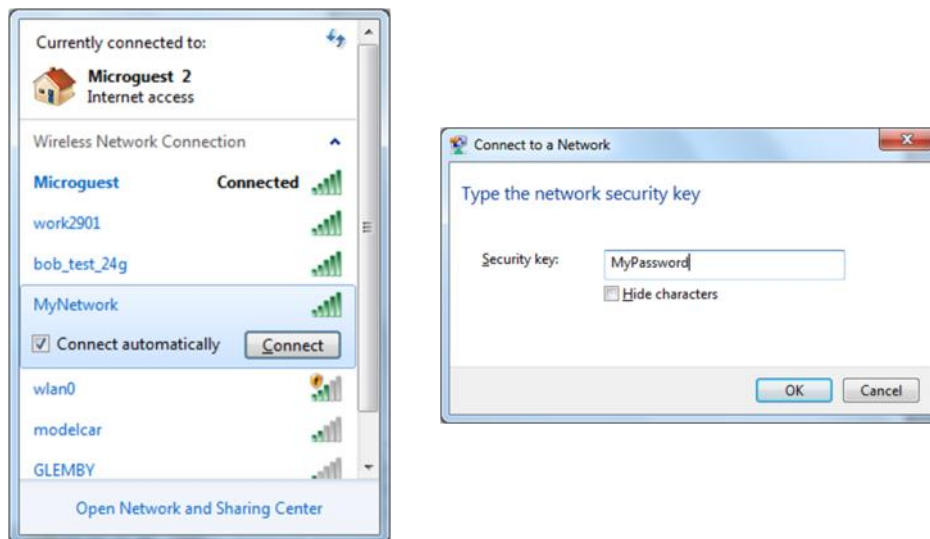
(Optional) Set a password for the WiFi, this example uses MyPassword

Click **Submit**.

## 2.0 Quick Start

### 2.3.2 Connecting to WiFi

- ✓ Now that the VIP4G has connection to the Cellular Carrier (See Section 2.2) and the WiFi has been set up (See Section 2.3), WiFi devices should be able to detect and connect to the VIP4G.
- ✓ On a WiFi enabled PC/Device, the SSID of MyNetwork, that was created in the last example should be visible. Connect to that SSID and enter the password.



- ✓ Once connected the status should change to connected, and network access should be enabled.



## 2.0 Quick Start

- ✓ The status of the WiFi connection should also be visible in the Wireless > Status tab in the WebUI as seen below.

The screenshot shows the WebUI of the Microhard Systems Inc. VIP4G device. The 'Wireless' tab is selected, and the 'Status' sub-tab is active. The interface displays the status of Radio 1, including General Status, Traffic Status, and Connection Status.

**Wireless Interfaces**

**Radio 1 Status**

**General Status**

MAC Address	Mode	SSID	Frequency Band	Radio Frequency	Security mode
00:80:48:77:E4:18	Access Point	MyNetwork	Dual-Band Mode	2.462	WPA2(PSK)

**Traffic Status**

Receive bytes	Receive packets	Transmit bytes	Transmit packets
83.912KB	488	117.016KB	659

**Connection Status**

MAC Address	Noise Floor (dBm)	SNR (dB)	RSSI (dBm)	TX CCQ (%)	RX CCQ (%)	TX Rate	RX Rate	Signal Level
48:5d:60:98:8c:94	-89	46	-49	92	96	54.0 MBit/s	54.0 MBit/s	100%

Stop Refreshing Interval: 20(s)

Copyright © 2012 Microhard Systems Inc. VIP4G-wifi

## 3.0 Hardware Features

### 3.1 VIP4G

The VIP4G is a fully-enclosed unit ready to be interfaced to external devices.



Image 3-1: Front View of VIP4G



Image 3-2: Rear View of VIP4G

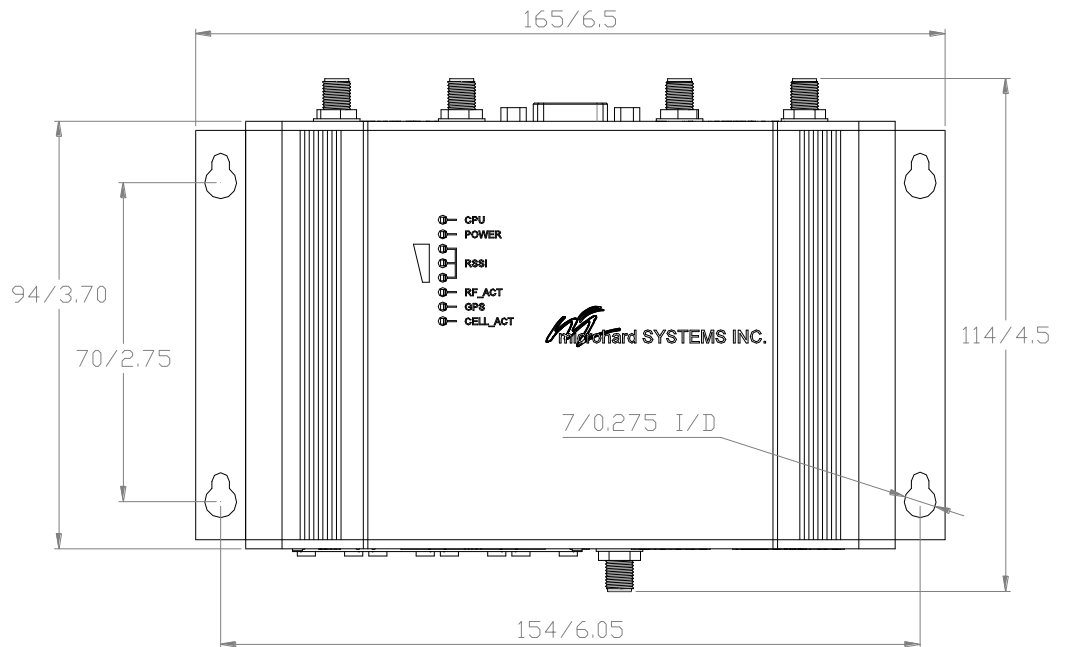
Any VIP4G may be configured as an Access Point (Router or Bridge), Station/Client, Repeater or Mesh Node. This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming very familiar and proficient with using the device: if you are familiar with one unit, you will be familiar with all units.

The VIP4G features:

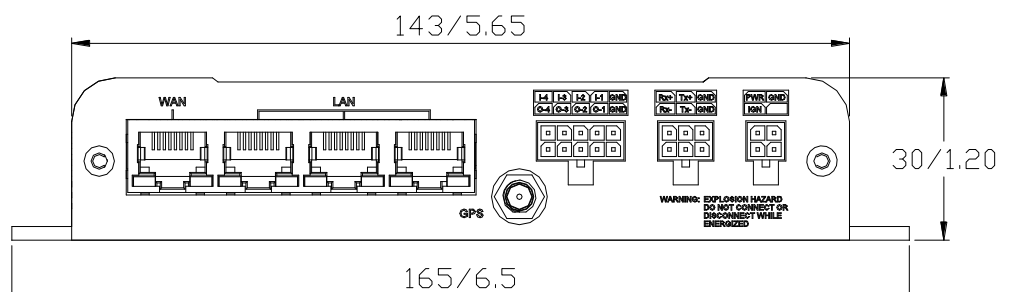
- Standard Connectors for:
  - 1 WAN Ethernet Ports (RJ45)
  - 3 LAN Ethernet Ports (RJ45)
  - Data Port (RS232/DB9)
  - 4-Pin: MATE-N-LOK Type Connector for Power
  - 6-Pin: MATE-N-LOK Type Connector for RS485 Data
  - 10-Pin: MATE-N-LOK Type Connector for Digital I/O
  - Cellular Antenna (SMA Female Antenna Connection x2)
  - WiFi Antenna (SMA Female Antenna Connection x2)
  - Built in GPS (SMA Female Antenna Connection)
- Status/Diagnostic LED's for CPU, POWER, RSSI, RF\_ACT, GPS, CELL\_ACT
- CFG Button for firmware recovery operations
- Mounting Holes

## 3.0 Hardware Features

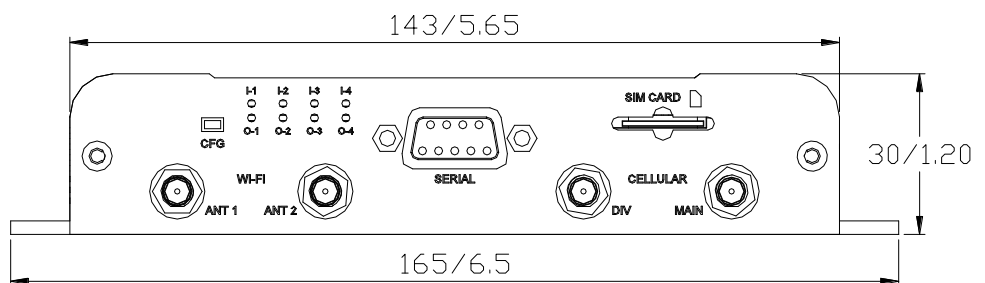
### 3.1.1 Mechanical Drawings



*Drawing 3-1: VIP Top View Dimensions*



*Drawing 3-2: VIP Front View Dimensions*



*Drawing 3-3: VIP Rear View Dimensions*

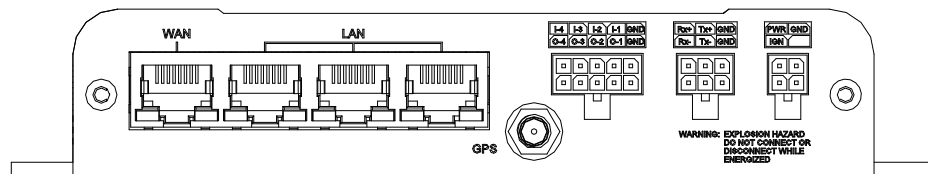
**Note: All dimension units: Millimeter & Inches (mm/inches)**

## 3.0 Hardware Features

### 3.1.2 Connections

#### 3.1.2.1 Front

On the front of the VIP4G Series are, from left to right:



Drawing 3-4: VIP4G Front View

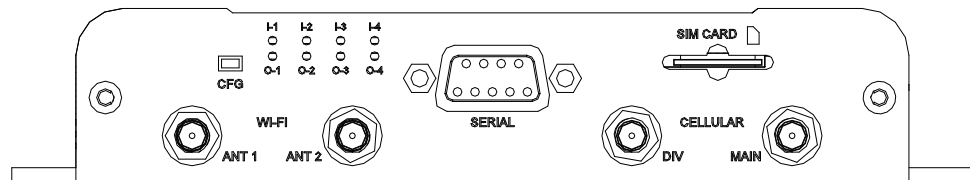
- WAN port
  - 10/100/1000 Ethernet RJ45 Connection.
- LAN port
  - 3x - 10/100/1000 Ethernet RJ45 Connection.
- GPS
  - SMA Female
- Digital I/O Connector 10-Pin: (Use AMP MATE-N-LOK PN# 1-794617-0)
  - I-4, I-3, I-2, I-1, GND
  - O-4, O-3, O-2, O-1, GND
- RS485/422 Connector 6-Pin: (Use AMP MATE-N-LOK PN# 794617-6)
  - Rx+, Tx+, GND
  - Rx-, Tx-, GND
- Power Connector 4-Pin: (Use AMP MATE-N-LOK PN# 794617-4)
  - PWR, GND



**Caution:** Using a power supply that does not provide proper voltage may damage the VIP4G unit.

## 3.0 Hardware Features

### 3.1.2.2 Rear



Drawing 3-5: VIP4G Rear View

#### CFG Button

Holding this button for 8 seconds while the VIP4G is powered up and running, will cause the unit to reset and load factory default settings:

**IP: 192.168.168.1 Subnet: 255.255.255.0 Gateway: 192.168.1.1**

**With these settings a web browser can be used to configure the unit.**

Holding this button depressed while powering-up the VIP4G will boot the unit into FLASH FILE SYSTEM RECOVERY mode. The default IP address for *system recovery (only - not for normal access to the unit)* is static: 192.168.1.39.

#### ANTENNA Connectors

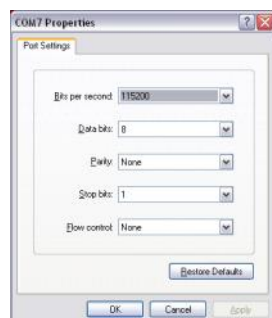
The VIP4G uses a female SMA antenna connector for the Cellular and WiFi antennas. Two antenna connections are provided for Wi-Fi, ANT1, and ANT2. Two connectors are also provided for Cellular, MAIN and DIV.

#### Digital I/O LED's

The I-1, I-2, I-3, and I-4 LED's indicate the status of the input pins on the digital I/O interface. The O-1, O-2, O-3 and O-4 LED's indicate the current state of the corresponding output relays.

#### Serial Port

The Serial port can be used for console type configuration (If disabled), or as a data communications port for RS232 Devices.



Default Console Port Settings:

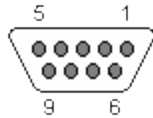
Bits per Second: 115,200  
Data Bits: 8  
Parity: None  
Stop bits: 1  
Flow control: None





## 3.0 Hardware Features

### Serial Port (Continued)



See **Appendix A** for a full description of the COM1 RS-232 interface functions.

Pin Name	No.	Description	In/Out
DCD	1	Data Carrier Detect	O
RXD	2	Receive Data	O
TXD	3	Transmit Data	I
DTR	4	Data Terminal Ready	I
SG	5	Signal Ground	
DSR	6	Data Set Ready	O
RTS	7	Request To Send	I
CTS	8	Clear To Send	O

Table 3-1: COM2 DB9 Pin Assignment

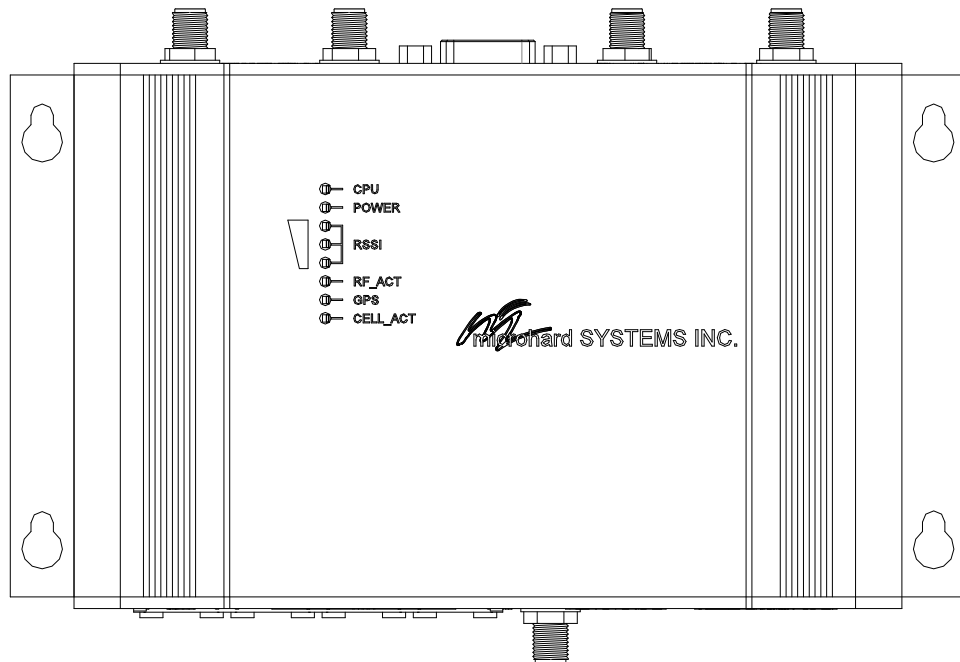
### SIM Card

This slot is used to install a SIM card provided by the cellular carrier to enable communication to their cellular network. Ensure the SIM card is installed properly by paying attention to the diagram printed above the SIM card slot.



## 3.0 Hardware Features

### 3.1.3 Indicators



*Drawing 3-6: VIP4G Indicators*

**CPU (Blue)**

ON indicates the CPU is running.

**POWER (Red)**

Illuminates when power is correctly applied to the unit.

**RSSI (3 LEDs)**

Indicate the received signal strength of the signal to the Cellular carrier. The number of LED's illuminated indicate the strength of the signal, with all 3 being illuminated representing a strong signal.

**RF-ACT**

The RF Activity LED illuminates when there is activity on the WiFi wireless interface.

**GPS**

Indicates that the GPS module is powered on and ready.

**CELL\_ACT**

The CELL Activity LED illuminates when there is cellular activity.

## 4.0 Configuration

### 4.0 Web User Interface

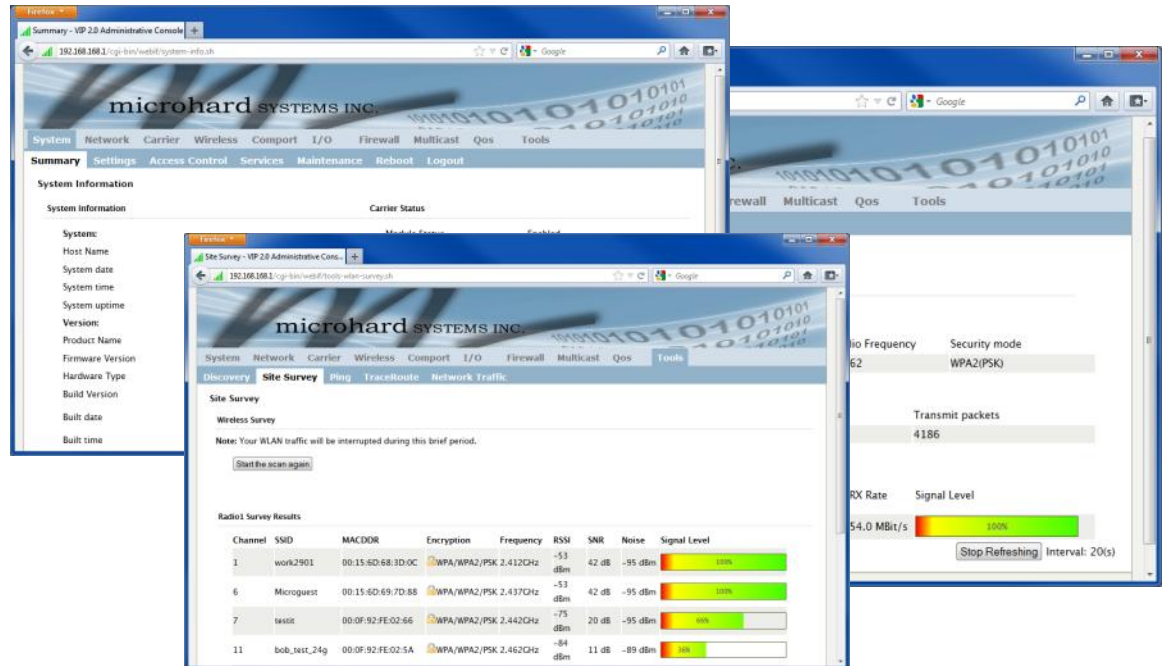


Image 6-1: WebUI

Initial configuration of an VIP4G using the Web User (Browser) Interface (Web UI) method involves the following steps:

- configure a static IP Address on your PC to 192.168.168.10 (or any address on the 192.168.168.X subnet other than the default IP of 192.168.168.1)
- connect a VIP4G LAN ETHERNET port to PC NIC card using an Ethernet cable
- apply power to the VIP4G and wait approximately 60 seconds for the system to load
- open a web browser and enter the factory default IP address of the unit: 192.168.168.1
- logon window appears; log on using default Username: **admin** Password: **admin**
- use the web browser based user interface to configure the VIP4G as required.
- refer to **Section 2.0: Quick Start** for step by step instructions.

In this section, all aspects of the Web Browser Interface, presented menus, and available configuration options will be discussed.

## 4.0 Configuration

### 4.0.1 Logon Window

Upon successfully accessing the VIP4G using a Web Browser, the Logon window will appear.



For security, do not allow the web browser to remember the User Name or Password.



It is advisable to change the login Password. Do not FORGET the new password as it cannot be recovered.

Image 4-2: Logon Window

The factory default User Name is: **admin**

The default password is: **admin**

Note that the password is case sensitive. It may be changed (discussed further along in this section), but once changed, if forgotten, may not be recovered.

When entered, the password appears as 'dots' as shown in the image below. This display format prohibits others from viewing the password.

The 'Remember my password' checkbox may be selected for purposes of convenience, however it is recommended to ensure it is deselected - particularly once the unit is deployed in the field - for one primary reason: security.

Image 4-3: Logon Window : Password Entry

## 4.0 Configuration

### 4.1 System

The main category tabs located at the top of the navigation bar separate the configuration of the VIP4G into different groups based on function. The System Tab contains the following sub menu's:

- Summary - Status summary of entire radio including network settings, version information, and radio connection status.
- Settings - Host Name, Default System Mode (Bridge or Router), System Time/Date, HTTP Port for the WebUI,
- Access Control - Change passwords, create new users
- Services - Enable/Disable RSSI LED's, SSH and Telnet services
- Maintenance - Version information, firmware Upgrades, reset to defaults, configuration backup and restore.
- Reboot - Remotely reboot the system.
- Logout - Logout of the current browser session.

#### 4.1.1 System > Summary

The System Summary screen is displayed immediately after initial login, showing a summary and status of all the functions of the VIP4G in a single display. This information includes System Status, Carrier Status, LAN & WAN network information, version info and WiFi radio status as seen below.

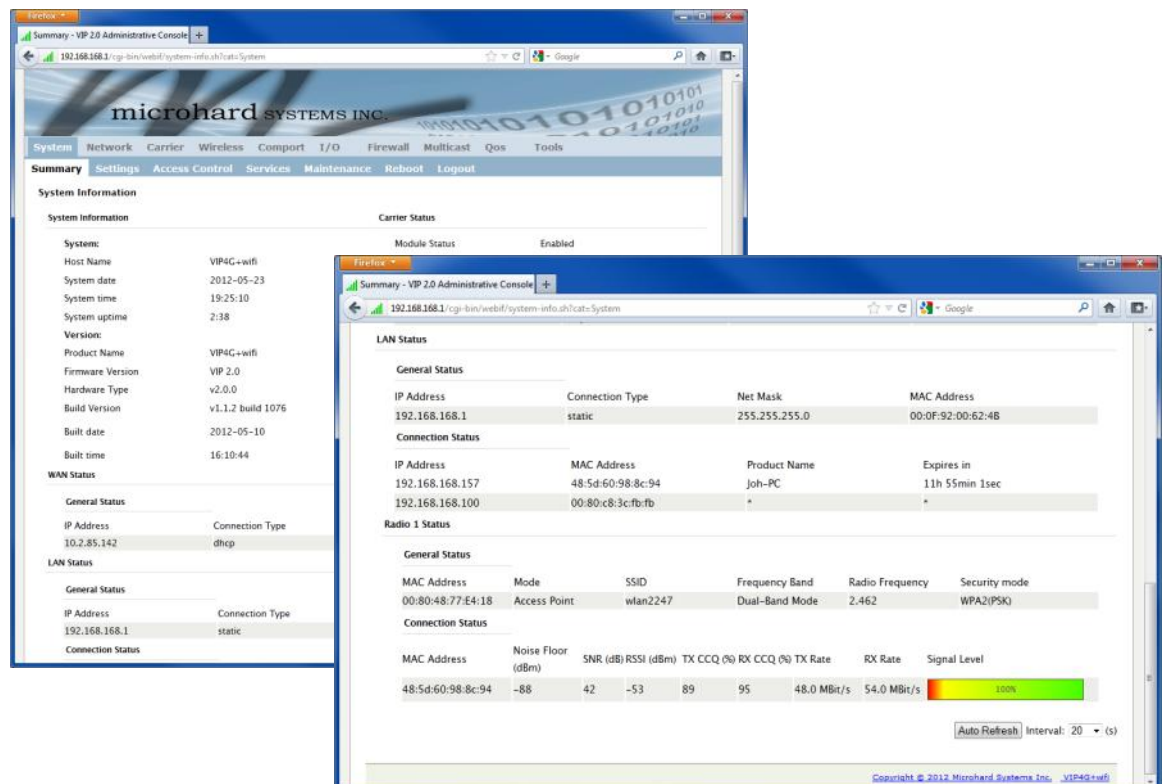


Image 4-4: System Info Window

## 4.0 Configuration

### 4.1.2 System > Settings

#### System Settings

Options available in the System Settings menu allow for the configuration of the Host Name.

The screenshot shows the 'System Settings' page in a web browser. The top navigation bar includes tabs for System, Network, Carrier, Wireless, Comport, I/O, Firewall, Multicast, Qos, VPN, and Tools. The 'Settings' tab is active. Below the navigation bar, there are sub-tabs: Summary, Settings, Access Control, Services, Maintenance, Reboot, and Logout. The 'Settings' sub-tab is selected. The main content area is titled 'System Settings'. It contains several sections: 'System Settings' with a 'Host Name' field set to 'VIP4G'; 'Time Settings' showing the current date (2012.07.31) and time (10:31:34), with a dropdown for 'Date and Time Setting Mode' set to 'Synchronize Date And Time Over Network', a 'Timezone' dropdown set to 'Mountain Time', a 'POSIX TZ String' field with 'MST7MDT,M3.2.0,M11.1.0', and 'NTP Server' and 'NTP Server Port' fields set to 'pool.ntp.org' and '123' respectively. There are also links for 'Remove NTP Server' and 'Add NTP Server'. The 'Web Configuration Settings' section has an 'HTTP Port' field set to '80' and an 'HTTP SSL' dropdown set to 'Off'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Image 4-5: System Settings > System Settings



The Host Name must not be confused with the **Network Name (SSID)** (Wireless Configuration menu). The Network Name **MUST** be exactly the same on each wireless device within a VIP4G network.

The Host Name is a convenient identifier for a specific VIP4G unit. This feature is most used when accessing units remotely: a convenient cross-reference for the unit's WAN IP address. This name appears when logged into a telnet session, or when the unit is reporting into Microhard NMS System.

#### Host Name

##### Values (characters)

**VIP4G+wifi (varies)**

up to 30 characters

## 4.0 Configuration

### Time Settings

The VIP4G can be set to use a local time source, thus keeping time on its own, or it can be configured to synchronize the date and time via a NTP Server. The options and menus available will change depending on the current setting of the Date and Time Setting Mode, as seen below.



Network Time Protocol (NTP) can be used to synchronize the time and date or computer systems with a centralized, referenced server. This can help ensure all systems on a network have the same time and date.

**Time Settings : Current Date(yyyy.mm.dd) 2011.04.01 Time(hh:mm:ss): 21:38:13**

Date and Time Setting Mode

Date (yyyy.mm.dd)

Time (hh:mm:ss)

**Time Settings : Current Date(yyyy.mm.dd) 2011.04.01 Time(hh:mm:ss): 05:16:37**

Date and Time Setting Mode

Timezone

POSIX TZ String

NTP Server

NTP Server Port

[Remove NTP Server](#)

[Add NTP Server](#)

Image 4-6: System Settings > Time Settings

### Date and Time Setting Mode

Select the Date and Time Setting Mode required. If set for 'Use Local Time' the unit will keep its own time and not attempt to synchronize with a network server. If 'Synchronize Date And Time Over Network' is selected, a NTP server can be defined.

#### Values (selection)

**Use Local Time Source**  
Synchronize Date And Time Over Network

### Date

The calendar date may be entered in this field. Note that the entered value is lost should the VIP4G lose power for some reason.

#### Values (yyyy-mm-dd)

**2011.04.01** (varies)

### Time

The time may be entered in this field. Note that the entered value is lost should the VIP Series lose power for some reason.

#### Values (hh:mm:ss)

**11:27:28** (varies)



## 4.0 Configuration

### Timezone

If connecting to a NTP time server, specify the timezone from the dropdown list.

Values (selection)

User Defined (or out of date)

### POSIX TZ String

This displays the POSIX TZ String used by the unit as determined by the timezone setting.

Values (read only)

(varies)

### NTP Server

Enter the IP Address or domain name of the desired NTP time server.

Values (address)

pool.ntp.org

### NTP Port

Enter the IP Address or domain name of the desired NTP time server.

Values (port#)

123

### Web Configuration Settings

The last section of the System Setting menu allows the configuration of the HTTP and HTTPS Ports used for the web server of the WEBUI.

Web Configuration Settings (Note: Changes will not take effect until the system is rebooted)	
HTTP Port	<input type="text" value="80"/>
HTTP SSL	<input type="button" value="On"/> ▼
HTTP SSL PORT	<input type="text" value="443"/>
<input type="button" value="OK, Reboot Now"/>	

Image 4-7: System Settings > Web Configuration Settings

### HTTP Port

The default web server port for the web based configuration tools used in the VIP is port 80. Change as required, but keep in mind that if a non standard port is used, it must be specified in a internet browser to access the unit. (example: http://192.168.168.1:8080)

Values (port#)

80

### HTTP Port

The secure web port (HTTPS) can be enabled or disabled using the **HTTP SSL** On/Off drop down menu. If enabled, the port used can be specified, the default is port 443.

Values (port#)

443

## 4.0 Configuration

### 4.1.3 System > Access Control

#### Password Change

The Password Change menu allows the password of the user 'admin' to be changed. The 'admin' username cannot be deleted, but additional users can be defined and deleted as required as seen in the Users menu below.

The screenshot displays the 'Access Control' configuration page. The 'Password Change' section is active, showing the 'admin' user selected. There are input fields for a new password and its confirmation, with a 'Change Passwd' button. Below this, the 'Users' section indicates no users are currently defined, with an 'Add User' button. A note specifies that changes will only take effect after a system reboot. The bottom of the page features 'Submit' and 'Cancel' buttons.

Image 4-8: Access Control > Password Change

#### New Password

Enter a new password for the 'admin' user. It must be at least 5 characters in length. The default password for 'admin' is 'admin'.

#### Values (characters)

admin

min 5 characters

#### Confirm Password

The exact password must be entered to confirm the password change, if there is a mistake all changes will be discarded.

#### Values (characters)

admin

min 5 characters



## 4.0 Configuration

### 4.1.3 System > Access Control

#### Users

Different users can be set up with customized access to the WebUI. Each menu or tab of the WebUI can be disabled on a per user basis as seen below.

**Users**

Test1 [Remove user Test1](#)

Add User: ( Note: Changes will not take effect until the system is rebooted )

Username

Password (min 5 characters)

Confirm Password

ACL User: Test1

**Comport**

Status

Com1

**Logout**

Logout

**Network**

Status

Networks

DHCP

SNMP

sdpServer

**Status**

DHCP Clients

Mesh

**System**

Info

Settings

Access Control

Maintenance

Reboot

**Tools**

Discovery

Site Survey

Ping

TraceRoute

Network Traffic

**Wireless**

Status

Radio1

Image 4-9: Access Control > Users

#### Username

Enter the desired username. Minimum or 5 character and maximum of 32 character. Changes will not take effect until the system has been restarted.

#### Values (characters)

(no default)  
Min 5 characters  
Max 32 characters

#### Password / Confirm Password

Passwords must be a minimum of 5 characters. The Password must be re-entered exactly in the Confirm Password box as well.

#### Values (characters)

(no default)  
min 5 characters

## 4.0 Configuration

### 4.1.4 System > Services

#### Available Services

Certain services in the VIP4G can be disabled or enabled for either security considerations or resource/power considerations. The Enable/Disable options are applied after a reboot and will take affect after each start up. The Start/Restart/Stop functions only apply to the current session and will not be retained after a power cycle.

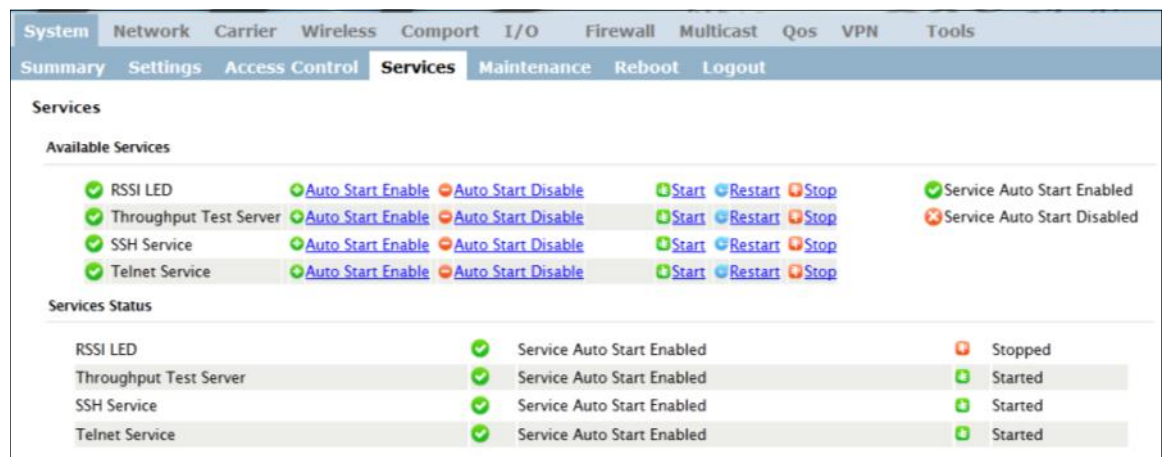


Image 4-10: System > Services

#### RSSI LED

The VIP4G has the ability to turn off the RSSI LED's. The RSSI value can still be read from the unit, but the status will not be visible on the unit itself .

#### Values (selection)

Enable / Disable

#### Throughput Test Server

For testing purposes the VIP4G has an internal lperf server that can be used to test unit performance. The user must install a lperf client to use this functionality.

#### Values (selection)

Enable / Disable

#### SSH Service

Using the SSH Service Enable/Disable function, you can disable the SSH service (Port 22) from running on the VIP4G.

#### Values (selection)

Enable / Disable

#### Telnet Service

Using the Telnet Service Enable/Disable function, you can disable the Telnet service (Port 23) from running on the VIP4G.

#### Values (characters)

Enable / Disable

## 4.0 Configuration

### 4.1.5 System > Maintenance

#### Version Information

Detailed version information can be found on this display. The Product Name, Firmware Version, Hardware Type, Build Version, Build Date and Build Time can all be seen here, and may be requested from Microhard Systems to provide technical support.

The screenshot shows the 'microhard SYSTEMS INC.' logo at the top. Below it is a navigation bar with tabs: System, Network, Carrier, Wireless, Comport, I/O, Firewall, Multicast, Qos, VPN, Tools. A secondary bar contains: Summary, Settings, Access Control, Services, Maintenance (selected), Reboot, Logout.

**System Maintenance**

**Version Information**

Product Name	Part No.	Serial No.	Hardware Type	Build Version	Build Date	Build Time
VIP4G_MHS123456	MHS123456	1012000	v2.0.0	v1.1.4 build 1089	2012-07-27	16:08:28

**Firmware Upgrade**

Erase Current Configuration: ☐ Keep ALL Configuration

Firmware Image:

Upgrade:

Image 4-11: Maintenance > Version Information / Firmware Upgrade

#### Firmware Upgrade

Occasional firmware updates may be releases by Microhard Systems which include fixes and new features. The firmware can be updated here wirelessly using the WebUI.

#### Erase Current Configuration

Check this box to erase the configuration of the VIP unit during the upgrade process. This will upgrade, and return the unit to factory defaults, including the default IP Addresses and passwords. Not checking the box will retain all settings during a firmware upgrade procedure.

#### Values (check box)

unchecked

#### Firmware Image

Use the Browse button to find the firmware file supplied by Microhard Systems. Select "Upgrade Firmware" to start the upgrade process. This can take several minutes.

#### Values (file)

(no default)

## 4.0 Configuration

### 4.1.5 System > Maintenance

#### Reset to Default

The VIP4G may be set back to factory defaults by using the Reset to Default option under System > Maintenance > Reset to Default. **\*Caution\*** - All settings will be lost!!!

The screenshot displays the 'Maintenance' configuration page for the VIP4G. It is divided into three main sections:

- Reset to Default:** Contains a 'Reset to Default Configuration' label and a 'Reset to Default' button.
- Backup Configuration:** Includes a text field 'Name this configuration' with the value 'VIP421' and a 'Backup Configuration' button.
- Restore Configuration:** Features a 'Restore Configuration file' label, a text input field, a 'Browse...' button, and a 'Check Restore File' button.

To the right of the 'Restore Configuration' section is a summary box titled 'Restore Configuration' showing the following details:

- The configuration looks good!
- Config file Name: AP1CONFIG
- Generated: Fri Apr 1 02:20:06 UTC 2011
- Vendor: 2010- Microhard Systems Inc.
- Product: VIP-VIP421
- Hardware Type: 2.0.0
- A 'Restore' button is located at the bottom of this box.

Image 4-12: Maintenance > Reset to Default / Backup & Restore Configuration

#### Backup & Restore Configuration

The configuration of the VIP4G can be backed up to a file at any time using the Backup Configuration feature. The file can then be restored using the Restore Configuration feature. It is always a good idea to backup any configurations in case of unit replacement. The configuration files cannot be edited offline, they are used strictly to backup and restore units.

#### Name this Configuration / Backup Configuration

Use this field to name the configuration file. The .config extension will automatically be added to the configuration file.

#### Restore Configuration file / Check Restore File / Restore

Use the 'Browse' button to find the backup file that needs to be restored to the unit. Use the 'Check Restore File' button to verify that the file is valid, and then the option to restore the configuration is displayed, as seen above.

## 4.0 Configuration

### 4.1.6 System > Reboot

The VIP can be remotely rebooted using the System > Reboot menu. As seen below a button 'OK, reboot now' is provided. Once pressed, the unit immediately reboots and starts its boot up procedure.

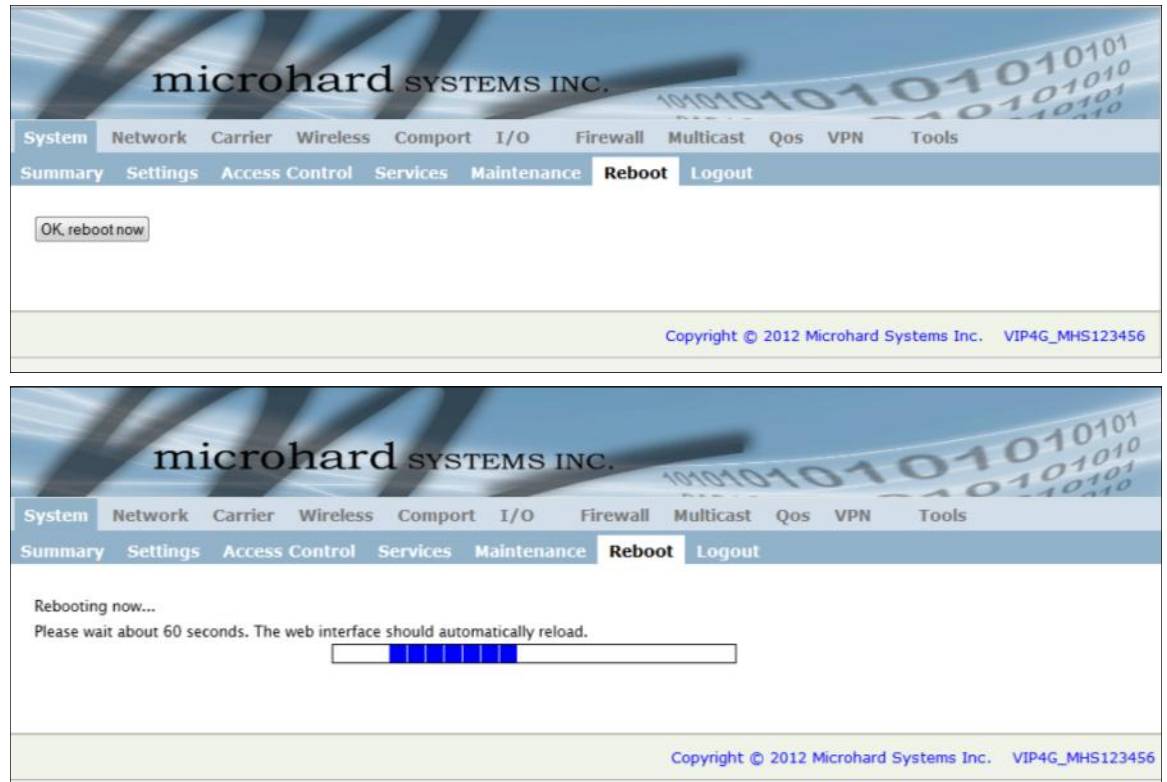


Image 4-13: System > Reboot



## 4.0 Configuration

### 4.1.7 System > Logout

The logout function allows a user to end the current configuration session and prompt for a login screen.

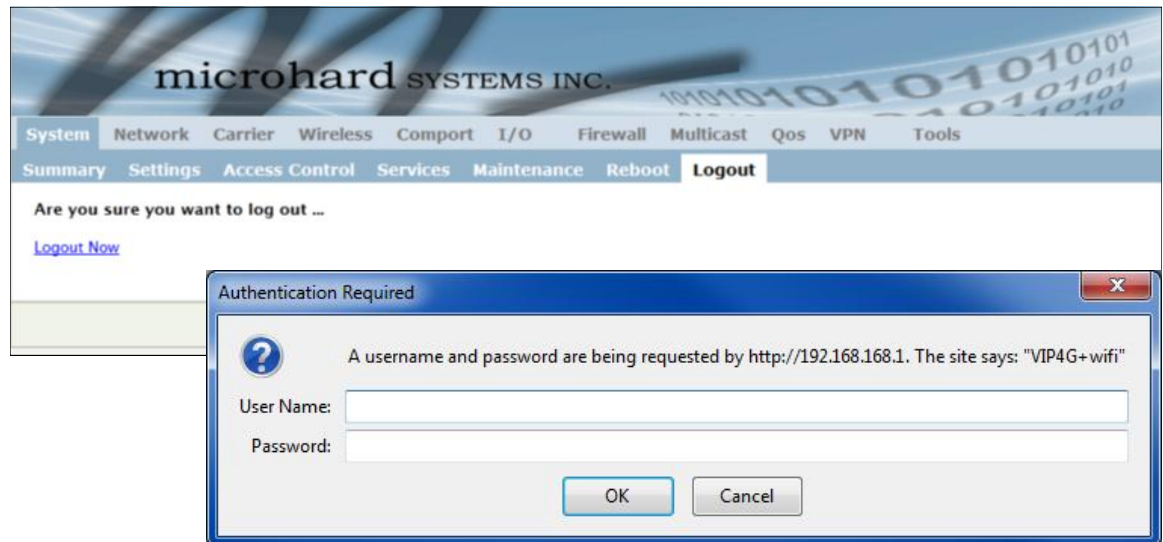


Image 4-14: System > logout

## 4.0 Configuration

### 4.2 Network

#### 4.2.1 Network > Status

The Network Status display gives a overview of the currently configured network interfaces including the Connection Type (Static/DHCP), IP Address, Net Mask, Default Gateway, DNS, and IPv4 Routing Table.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
Status	Networks	DHCP	VLAN	Routes	GRE	SNMP	sdpServer			
Network Status										
LAN Port Status										
General Status										
IP Address			Connection Type			Net Mask		MAC Address		
192.168.168.1			static			255.255.255.0		00:0F:92:00:00:00		
Traffic Status										
Receive bytes			Receive packets			Transmit bytes		Transmit packets		
251.223KB			3048			4.05793MB		3930		
WAN Port Status										
General Status										
IP Address			Connection Type			Net Mask		MAC Address		
N/A			dhcp			N/A		00:0F:92:01:00:00		
Traffic Status										
Receive bytes			Receive packets			Transmit bytes		Transmit packets		
1.952KB			11			184.536KB		475		
Default Gateway										
Gateway			25.88.93.253							
DNS										
DNS Server(s)			64.71.255.198 64.71.255.253							
IPv4 Routing Table										
Destination			Gateway			Netmask		Flags	Metric	Ref Use Interface
25.88.93.252			0.0.0.0			255.255.255.252		U	0	0 0 (br-wan2)
192.168.168.0			0.0.0.0			255.255.255.0		U	0	0 0 (br-lan)
0.0.0.0			25.88.93.253			0.0.0.0		UG	0	0 0 (br-wan2)

Image 4-15: Network > Network Status

## 4.0 Configuration

### 4.2.2 Network > Networks

#### Network Configuration

The Networks menu is where the local Ethernet interfaces can be configured.

The screenshot displays the 'Network Configuration' page of the microhard SYSTEMS INC. web interface. The top navigation bar includes 'System', 'Network', 'Carrier', 'Wireless', 'Comport', 'I/O', 'Firewall', 'Multicast', 'Qos', 'VPN', and 'Tools'. The 'Networks' sub-menu is active, showing options like 'Status', 'Networks', 'DHCP', 'VLAN', 'Routes', 'GRE', 'SNMP', and 'sdpServer'. The main content area is titled 'Network Configuration' and is divided into two main sections: 'LAN Configuration' and 'WAN Configuration'. Each section contains fields for 'Connection Type' (set to 'Static IP'), 'IP Address', 'Netmask', 'Default Gateway', 'IPv6 Address', and 'Default IPv6 Gateway'. The 'LAN Configuration' section has the IP Address set to '192.168.168.1' and Netmask set to '255.255.255.0'. Below each configuration section is a 'LAN DNS Servers' and 'WAN DNS Servers' section, each with an 'Add' button.

Image 4-16: Network > Network Configuration



## 4.0 Configuration

### LAN Configuration



**DHCP:** Dynamic Host Configuration Protocol may be used by networked devices (Clients) to obtain unique network addresses from a DHCP server.

**Advantage:**

Ensures unique IP addresses are assigned, from a central point (DHCP server) within a network.

**Disadvantage:**

The address of a particular device is not 'known' and is also subject to change.

STATIC addresses must be tracked (to avoid duplicate use), yet they may be permanently assigned to a device.



Within any IP network, each device must have its own unique IP address.



A SUBNET MASK is a bit mask that separates the network and host (device) portions of an IP address.

The 'unmasked' portion leaves available the information required to identify the various devices on the subnet.

The LAN submenu, along with the Wireless Configuration settings, are the minimum required when implementing any VIP4G network. It must be defined if the unit is to be either:

- assigned an IP address (by a DHCP server), or
- given a static (unchanging) IP address.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
Status	<b>Networks</b>	DHCP	VLAN	Routes	GRE	SNMP	sdpServer			
<b>Network Configuration</b>										
<b>LAN Configuration</b>										
Connection Type		Static IP ▾								
IP Address		192.168.168.1								
Netmask		255.255.255.0								
Default Gateway										
IPv6 Address										
Default IPv6 Gateway										

Image 4-17: Network Configuration > LAN Configuration

#### Connection Type

##### Values (selection)

DHCP  
Static

This selection determines if the VIP will obtain an IP address from a DHCP server on the attached network, or if a static IP address will be entered. If a Static IP Address is chosen, the fields that follow must also be populated.

#### IP Address

##### Values (IP Address)

192.168.168.1

If 'Static' Connection Type is selected, a valid IPv4 Address for the network being used must be entered in the field. If 'DHCP' is chosen this field will not appear and it will be populated automatically from the DHCP server.

#### Netmask

##### Values (IP Address)

255.255.255.0

If 'Static' Connection Type is selected, the Network Mask must be entered for the Network. If 'DHCP' is chosen this field will not appear and it will be populated automatically from the DHCP server.

## 4.0 Configuration



A GATEWAY is a point within a network that acts as an entrance to another network.

In typical networks, a router acts as a gateway.



DNS: Domain Name Service is an Internet service that translates easily-remembered domain names into their not-so-easily-remembered IP addresses.

Being that the Internet is based on IP addresses, without DNS, if one entered the domain name `www.microhardcorp.com` (for example) into the URL line of a web browser, the website 'could not be found'.

### Default Gateway

#### Values (IP Address)

(no default)

If the VIP4G is integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway's IP address will be entered into this field. If there is a DHCP server on the network, and the Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

A simple way of looking at what the gateway value should be is: If a device has a packet of data it does not know where to send, send it to the gateway. If necessary - and applicable - the gateway can forward the packet onwards to another network.

### LAN DNS Servers

#### Values (IP Address)

(no default)

DNS (Domain Name Service) Servers are used to resolve domain names into IP addresses. If the Connection Type is set for DHCP the DHCP server will populate this field and the value set can be viewed on the Network > Status page.

### WAN Configuration

The configuration of the WAN interface is identical to the LAN interface, so refer back to the previous section for information about the Connection Type, IP Address, Netmask, Default Gateway and WAN DNS Servers.

WAN Configuration	
Connection Type	Static IP ▼
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
IPv6 Address	<input type="text"/>
Default IPv6 Gateway	<input type="text"/>
WAN DNS Servers	
<input type="text"/>	<input type="button" value="Add"/>

Image 4-18: Network Configuration > WAN Configuration

## 4.0 Configuration

### 4.2.3 Network > DHCP



**DHCP:** Dynamic Host Configuration Protocol may be used by networked devices (Clients) to obtain unique network addresses from a DHCP server.

**Advantage:**

Ensures unique IP addresses are assigned, from a central point (DHCP server) within a network.

**Disadvantage:**

The address of a particular device is not 'known' and is also subject to change.

STATIC addresses must be tracked (to avoid duplicate use), yet they may be permanently assigned to a device.



Prior to enabling this service, verify that there are no other devices - either wired (e.g. LAN) or wireless (e.g. another VIP Series unit) with an active DHCP SERVER service. (The Server issues IP address information at the request of a DHCP Client, which receives the information.)

### DHCP Configuration > LAN DHCP

A VIP4G may be configured to provide dynamic host control protocol (DHCP) service to all attached (either wired or wireless (WiFi)-connected) devices. By default the DHCP service is enabled, so devices that are connected to the physical Ethernet LAN ports, as well as any devices that are connected by WiFi will be assigned an IP by the VIP4G.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools												
Status	Networks	DHCP	VLAN	Routes	GRE	SNMP	sdpServer															
<b>DHCP Configuration</b>																						
<b>LAN DHCP</b>																						
DHCP <input checked="" type="radio"/> On <input type="radio"/> Off																						
Start <input type="text" value="192.168.168.100"/>																						
End <input type="text" value="192.168.168.250"/>																						
Lease Time (in minutes) <input type="text" value="720"/>																						
<b>Static IP addresses (for DHCP)</b>																						
<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>											Name	MAC Address	IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>						
Name	MAC Address	IP Address																				
<input type="text"/>	<input type="text"/>	<input type="text"/>																				
<b>Static Addresses</b>																						
<table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Name</th> <th>NetStatus</th> </tr> </thead> <tbody> <tr> <td>48:5D:60:98:8C:94</td> <td>192.168.168.150</td> <td>Laptop</td> <td><a href="#">Remove Laptop</a></td> </tr> </tbody> </table>											MAC Address	IP Address	Name	NetStatus	48:5D:60:98:8C:94	192.168.168.150	Laptop	<a href="#">Remove Laptop</a>				
MAC Address	IP Address	Name	NetStatus																			
48:5D:60:98:8C:94	192.168.168.150	Laptop	<a href="#">Remove Laptop</a>																			
<b>Active DHCP Leases</b>																						
<table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Name</th> <th>Expires in</th> </tr> </thead> <tbody> <tr> <td>98:03:d8:c5:52:18</td> <td>192.168.168.110</td> <td>Pauls-iPhone</td> <td>11h 59min 52sec</td> </tr> <tr> <td>00:80:c8:3c:fb:fb</td> <td>192.168.168.184</td> <td>DMKT0002-2</td> <td>11h 53min 59sec</td> </tr> </tbody> </table>											MAC Address	IP Address	Name	Expires in	98:03:d8:c5:52:18	192.168.168.110	Pauls-iPhone	11h 59min 52sec	00:80:c8:3c:fb:fb	192.168.168.184	DMKT0002-2	11h 53min 59sec
MAC Address	IP Address	Name	Expires in																			
98:03:d8:c5:52:18	192.168.168.110	Pauls-iPhone	11h 59min 52sec																			
00:80:c8:3c:fb:fb	192.168.168.184	DMKT0002-2	11h 53min 59sec																			
<div>Submit « Cancel «</div>																						

Image 4-19: Network > DHCP Configuration

#### DHCP

#### Values (selection)

On / Off

#### Start / End IP Address Range

#### Values (IP Address)

(varies)

The option is used to enable or disable the DHCP service for devices connected to the LAN Port and devices connected through a Wireless connection. This includes VIP connected as clients and other wireless devices such as 802.11 connections.

Select the range for the DHCP assignable addresses. The first octets of the subnet will be pre-set based on the LAN IP configuration, and can not be changed.

## 4.0 Configuration

### Lease Time

The DHCP lease time is the amount of time before a new request for a network address must be made to the DHCP Server.

Values (minutes)

(minutes)

### DHCP Configuration > Static IP Addresses (for DHCP)

In some applications it is important that specific devices always have a predetermined IP address. This section allows for MAC Address binding to a IP Address, so that whenever the device that has the specified MAC address, will always get the selected IP address. In this situation, all attached (wired or wireless) devices can all be configured for DHCP, but still get a known IP address.

### Name

The name field is used to give the device a easily recognizable name.

Values (characters)

(no default)

### MAC Address

Enter in the MAC address of the device to be bound to a set IP address. Set the IP Address in the next field. Must use the format: AB:CD:DF:12:34:D3. It is not case sensitive, but the colons must be present.

Values (MAC Address)

(no default)

### IP Address

Enter the IP Address to be assign to the device specified by the MAC address above.

Values (IP Address)

(minutes)

### Static Addresses

This section displays the IP address and MAC address currently assigned through the DHCP service, that are bound by it's MAC address. Also shown is the Name, and the ability to remove the binding by clicking "Remove \_\_\_\_\_".

### Active DHCP Leases

This section displays the IP Addresses currently assigned through the DHCP service. Also shown is the MAC Address, Name and Expiry time of the lease for reference.

## 4.0 Configuration

### 4.2.4 Network > VLAN



**VLAN:** Virtual LAN, used to separate networks logically, while utilizing a common infrastructure. This is useful to filter out any unwanted, or unneeded traffic, resulting in a more efficient use bandwidth, and enhanced security.

#### Network VLAN Configuration

The VIP4G has support to participate in VLAN networking, enabling the virtual separation of networks. The VIP4G allows the tagging, un-tagging and filtering of Ethernet frames on the LAN & Wireless Ports.

Image 4-20: Network > VLAN

#### VLAN

To enable the use of VLAN, select the "Enable" VLAN option from the drop down box. If disabled, the VIP will transmit/receive all traffic transparently, regardless of VLAN configuration on attached switched and routers.

#### Values (selection)

**Disabled** / Enabled

## 4.0 Configuration

### Management VLAN

Specify which VLAN is used as the management VLAN. By default only vlan1 is listed until additional VLANs are created in the VLAN Configuration section below.

#### Values (selection)

vlan1

### VLAN1 Configuration

VLAN1 is the native VLAN for VIP4G. By default, all traffic will be added to VLAN1 unless specified otherwise by adding additional VLAN(s) for the LAN/Wireless Interfaces.

### Description

Add a name or other description to VLAN1

#### Values (characters)

native

### WAN

Specify if traffic on the WAN interface is to join VLAN1

#### Values (selection)

Join VLAN / No VLAN

### Radio1

Specify if traffic on the Wireless interface is to join VLAN1

#### Values (selection)

Join VLAN / No VLAN

### VLANs Configuration

Create VLANs and assign LAN / Wireless Interface as required.

### VLAN ID

Assign the VLAN ID. Valid VLAN IDs range from 2 - 4094

#### Values (value)

*Varies (2-4094)*

### Description

The description field allows the assignment of a name or description of the VLAN for easy reference.

#### Values (characters)

*varies*

### WAN / Radio1

Specify if traffic on the Wireless or LAN interface is to Join (allow to pass through), and/or for the Ethernet frames to be Tagged for the current VLAN.

#### Values (selection)

Join VLAN / No VLAN



## 4.0 Configuration

### 4.2.5 Network > Routes

#### Static Route Configuration

It may be desirable to have devices on different subnets to be able to talk to one another. This can be accomplished with either a static route being defined, or in the case of being able to automatically share routing information using RIPv2, dynamic routing can be configured.

Image 4-21: Network > Routes

#### Name

Routes can be names for easy reference, or to describe the route being added.

Values (characters)

(no default)

#### Destination

Enter the network IP address for the destination.

Values (IP Address)

(192.168.168.0)



## 4.0 Configuration

### Gateway

Specify the Gateway used to reach the network specified above.

Values (IP Address)

192.168.168.1

### Netmask

Enter the Netmask for the destination network.

Values (IP Address)

255.255.255.0

### Metric

In some cases there may be multiple routes to reach a destination. The Metric can be set to give certain routes priority, the lower the metric is, the better the route. The more hops it takes to get to a destination, the higher the metric.

Values (Integer)

255.255.255.0

### Interface

Define the exit interface. Is the destination a device on the LAN, or the WAN?

Values (Selection)

LAN  
WAN  
None

### Dynamic Route Configuration

The VIP4G can support Dynamic Routing on the LAN and Wireless Ports. The VIP4G will communicate with other devices running RIPv2 to automatically populate a routing table.

### Route Mode

Enable /Disable Dynamic Routing.

Values (Selection)

Enable  
Disable

### Name

The Name field allows a user to give the Network a name for reference.

Values (Characters)

(varies)

### Network

Specify the IP and Subnet of any networks that are to be advertised to other devices via dynamic routing.

Values (IP/Subnet)

(varies)

## 4.0 Configuration

### 4.2.5 Network > GRE

#### GRE Configuration

The VIP4G supports GRE (Generic Routing Encapsulation) Tunneling which can encapsulate a wide variety of network layer protocols not supported by traditional VPN. This allows IP packets to travel from one side of a GRE tunnel to the other without being parsed or treated like IP packets.

The screenshot shows the 'GRE' tab selected in the 'Network' section. The 'GRE Configuration Summary' table lists one configured GRE tunnel.

No.	Name	Status	Multicast Status	ARP Status	TTL	Local IP	Local WAN	Remote Subnet	Remote WAN	Action
1	gre	Enable	Enable	Enable	255	0.0.0.0/0	0.0.0.0	0.0.0.0/0	0.0.0.0	<a href="#">Remove</a> <a href="#">Edit</a>

Image 4-22: Network > GRE

The screenshot shows the 'GRE Configuration' form with various settings and a summary table.

**GRE Configuration**

Name:

Local Status:

Multicast:

ARP:

TTL:

Local Subnet Gateway:

Local WAN IP:

Remote Subnet:

Remote Wan:

**GRE Configuration Summary**

No.	Name	Status	Multicast Status	ARP Status	TTL	Local IP	Local WAN	Remote Subnet	Remote WAN	Action
1	gre	Enable	Enable	Enable	255	0.0.0.0/0	0.0.0.0	0.0.0.0/0	0.0.0.0	<a href="#">Remove</a> <a href="#">Edit</a>

Image 4-23: Network > GRE

Name

Each GRE tunnel must have a unique name. Up to 10 GRE tunnels are supported by the IPn3G.

Values (Chars(32))

gre

## 4.0 Configuration

### GRE Tunnel Local Status

Enable / Disable the GRE Tunnel.

Values (selection)

Disable / **Enable**

### Multicast

Enable / Disable Multicast support over the GRE tunnel.

Values (selection)

Disable / **Enable**

### ARP

Enable / Disable ARP (Address Resolution Protocol) support over the GRE tunnel.

Values (selection)

Disable / **Enable**

### TTL

Set the TTL (Time-to-live) value for packets traveling through the GRE tunnel.

Values (value)

1 - **255**

### Local Subnet Gateway

This is the IP Address of the local network.

Values (IP Address)

(varies)

### Local WAN IP

This is the WAN IP Address of the VIP4G, this field should be populated with the current WAN IP address.

Values (IP Address)

(varies)

### Remote Subnet

The is the IP Address of the remote network, on the remote side of the GRE Tunnel.

Values (IP Address)

(varies)

### Remote WAN

Enter the WAN IP Address of the VIP4G or other GRE supported device in which a tunnel is to be created with.

Values (IP Address)

(varies)

## 4.0 Configuration

### 4.2.7 Network > SNMP

The VIP4G may be configured to operate as a Simple Network Management Protocol (SNMP) agent. Network management is most important in larger networks, so as to be able to manage resources and measure performance. SNMP may be used in several ways:



SNMP: Simple Network Management Protocol provides a method of managing network devices from a single PC running network management software.

Managed networked devices are referred to as SNMP agents.

- configure remote devices
- monitor network performance
- detect faults
- audit network usage
- detect authentication failures

A SNMP management system (a PC running SNMP management software) is required for this service to operate. This system must have full access to the VIP4G. Communications is in the form of queries (information requested by the management system) or traps (information initiated at, and provided by, the SNMP agent in response to predefined events).

Objects specific to the VIP4G are hosted under private enterprise number **21703**.

An object is a variable in the device and is defined by a Management Information Database (MIB). Both the management system and the device have a copy of the MIB. The MIB in the management system provides for identification and processing of the information sent by a device (either responses to queries or device-sourced traps). The MIB in the device relates subroutine addresses to objects in order to read data from, or write data to, variables in the device.

An SNMPv1 agent accepts commands to retrieve an object, retrieve the next object, set an object to a specified value, send a value in response to a received command, and send a value in response to an event (trap).

SNMPv2c adds to the above the ability to retrieve a large number of objects in response to a single request.

SNMPv3 adds strong security features including encryption; a shared password key is utilized. Secure device monitoring over the Internet is possible. In addition to the commands noted as supported above, there is a command to synchronize with a remote management station.

The pages that follow describe the different fields required to set up SNMP on the VIP4G. MIBs may be requested from Microhard Systems Inc.

Custom MIBs can be obtained by contacting Microhard Systems Inc. The MIB file can change when new features are added, so it is best to contact Microhard Systems Inc. for the complete and latest MIB file for the VIP4G.

## 4.0 Configuration

### SNMP Settings

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
Status	Networks	DHCP	VLAN	Routes	GRE	<b>SNMP</b>	sdpServer			

**SNMP Settings**

**SNMP Settings**

SNMP Operation Mode
☐ Disable
☒ V1&V2c&V3

Read Only Community Name

Read Write Community Name

SNMP V3 User Name

V3 User Read Write Limit
☒ Read Only
☐ Read Write

V3 User Authentication Level

V3 Authentication Password

V3 Privacy Password

SNMP Trap Version

Auth Failure Traps
☒ Disable
☐ Enable

Trap Community Name

Trap Manage Host IP

Image 4-24: Network > SNMP

#### SNMP Operation Mode

If disabled, an SNMP service is not provided from the device. Enabled, the device - now an SNMP agent - can support SNMPv1, v2, & v3.

#### Values (selection)

**Disable / V1&V2c&V3**

#### Read Only Community Name

Effectively a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ priority.

#### Values (string)

**public**

#### Read Only Community Name

Also a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ/WRITE priority.

#### Values (string)

**private**

#### SNMP V3 User Name

Defines the user name for SNMPv3.

#### Values (string)

**V3user**

## 4.0 Configuration

### V3 User Read Write Limit

Defines accessibility of SNMPv3; If Read Only is selected, the SNMPv3 user may only read information; if Read Write is selected, the SNMPv3 user may read and write (set) variables.

#### Values (selection)

**Read Only** / Read Write

### V3 User Authentication Level

Defines SNMPv3 user's authentication level:

NoAuthNoPriv: No authentication, no encryption.

AuthNoPriv: Authentication, no encryption.

AuthPriv: Authentication, encryption.

#### Values (selection)

**NoAuthNoPriv**

AuthNoPriv

AuthPriv

### V3 User Authentication Password

SNMPv3 user's authentication password. Only valid when V3 User Authentication Level set to AuthNoPriv or AuthPriv.

#### Values (string)

00000000

### V3 User Privacy Password

SNMPv3 user's encryption password. Only valid when V3 User Authentication Level set to AuthPriv (see above).

#### Values (string)

00000000

### SNMP Trap Version

Select which version of trap will be sent should a failure or alarm condition occur.

#### Values (string)

**V1 Traps**      V2 Traps  
V3 Traps      V1&V2 Traps  
V1&V2&V3 Traps

### Auth Failure Traps

If enabled, an authentication failure trap will be generated upon authentication failure.

#### Values (selection)

**Disable** / Enable

### Trap Community Name

The community name which may receive traps.

#### Values (string)

TrapUser

### Trap Manage Host IP

Defines a host IP address where traps will be sent to (e.g. SNMP management system PC IP address).

#### Values (IP Address)

0.0.0.0



## 4.0 Configuration

### 4.2.8 Network > sdpServer

#### sdpServer Settings

Microhard Radio employ a discovery service that can be used to detect other Microhard Radio's on a network. This can be done using a stand alone utility from Microhard System's called 'IP Discovery' or from the Tools > Discovery menu. The discovery service will report the MAC Address, IP Address, Description, Product Name, Firmware Version, Operating Mode, and the SSID.



Image 4-25: Network > sdpServer Settings

#### Discovery Service Status

Use this option to disable or enable the discovery service.

##### Values (selection)

Disable / **Discoverable** /  
Changable

#### Server Port Settings

Specify the port running the discovery service on the VIP4G unit.

##### Values (Port #)

20097



## 4.0 Configuration

### 4.3 Carrier

#### 4.3.1 Carrier > Status

The Carrier Status window provides complete overview information related to the Cellular Carrier portion of the VIP4G. A variety of information can be found here, such as Activity Status, Network (Name of Wireless Carrier connected) , Data Service Type(2G/3G etc), Frequency band, Phone Number etc.



Image 4-26: Carrier > Status

Not all statistics parameters displayed are applicable.

The Received and Transmitted bytes and packets indicate the respective amount of data which has been moved through the radio.

The Error counts reflect those having occurred on the wireless link.

## 4.0 Configuration

### 4.3 Carrier

#### 4.3.2 Carrier > Settings

The parameters within the Carrier Configuration menu must be input properly; they are the most basic requirement required by your cellular provider for network connectivity.

microhard SYSTEMS INC.

System Network **Carrier** Wireless Comport I/O Firewall Multicast Qos VPN Tools

Status **Settings** Keepalive Traffic Watchdog Dynamic DNS

**Carrier Configuration**

Configuration

Carrier status

APN

SIM Pin

Technologies Type

Technologies Mode

Data Call Parameters

Primary DNS Address

Secondary DNS Address

Primary NetBIOS Name Server

Secondary NetBIOS Server

IP Address

Authentication

User Name

Password

Image 4-27: Carrier > Carrier

#### Carrier Status

Carrier Status is used to Enable or Disable the connection to the Cellular Carrier. By default this option is enabled.

#### Values (Selection)

Enable / Disable

#### APN (Access Point Name)

The APN is required by every Carrier in order to connect to their networks. The APN defines the type of network the VIP4G is connected to and the service type. Most Carrier have more than one APN, usually many, dependant on the types of service offered.

#### Values (Selection)

Enable / Disable

## 4.0 Configuration

### SIM Pin

The SIM Pin is required for some international carriers. If supplied and required by the cellular carrier, enter the SIM Pin here.

#### Values (characters)

(none)

### Technologies Type

Set to ALL by default, the Technologies field allows the selection of 3GPP technologies (LTE), and or 3GPP2 technology (CDMA).

#### Values (Selection)

ALL  
3GPP  
3GPP2

### Technologies Mode

The Technologies Mode option allows a user the ability to specify what type of Cellular networks to connect to.

#### Values (Selection)

AUTO  
LTE Only  
WCDMA Only  
GSM Only

### Data Call Parameters

Sets the modems connect string if required by the carrier. Not usually required in North America.

#### Values (string)

(none)

### Primary DNS Address

If let blank the VIP4G will use the DNS server as specified automatically by the service provider.

#### Values (IP Address)

(none)

### Secondary DNS Address

If let blank the VIP4G will use the DNS server as specified automatically by the service provider.

#### Values (IP Address)

(none)

### Primary NetBIOS Name Server

Enter the Primary NetBIOS Name Server if required by the carrier.

#### Values (IP Address)

(none)

### Secondary NetBIOS Name Server

Enter the Secondary NetBIOS Name Server if required by the carrier.

#### Values (IP Address)

(none)

## 4.0 Configuration

### IP Address

In some cases the Static IP address must be entered in this field if assigned by a wireless carrier. In most cases the IP will be read from the SIM card and this field should be left at the default value.

#### Values (IP Address)

(none)

### Authentication

Sets the authentication type required to negotiate with peer.

#### Values (Selection)

PAP - Password Authentication Protocol.

CHAP - Challenge Handshake Authentication Protocol.

**Device decide (AUTO)**

PAP

CHAP

### User Name

A User Name may be required for authentication to a remote peer. Although usually not required for dynamically assigned IP addresses from the wireless carrier, but required in most cases for static IP addresses. Varies by carrier.

#### Values (characters)

Carrier/peer dependant

### Password

Enter the password for the user name above. May not be required by some carriers, or APN's

#### Values (characters)

Carrier/peer dependant

## 4.0 Configuration

### 4.3 Carrier

#### 4.3.3 Carrier > Keepalive

The Keep alive tab allows for the configuration of the keep alive features of the VIP4G. The VIP4G can either do a ICMP or HTTP keep alive by attempting to reach a specified address at a regular interval. If the VIP4G cannot reach the intended destination, it will reset the unit in an attempt to obtain a new connection to the carrier.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
Status	Settings	Keepalive	Traffic Watchdog	Dynamic DNS						
<b>Keepalive Configuration</b> Configuration Keep alive status: <input type="text" value="Enable"/> Type: <input type="text" value="ICMP"/> Host Name: <input type="text" value="8.8.8.8"/> Interval (60 ~ 60000): <input type="text" value="300"/> (s) Count: <input type="text" value="10"/>										

Image 4-28: Carrier > Keepalive

#### Keep Alive Status

Enable or Disable the keep alive functions in the VIP4G.

Values (Selection)

Enable / Disable

#### Type

Select the type of keep alive used. ICMP uses a "ping" to reach a select destination.

Values (Selection)

ICMP / HTTP

#### Host Name

Specify a IP Address or Domain that is used to test the VIP4G connection.

Values (IP or Domain)

8.8.8.8

#### Interval

The Interval value determines the frequency, or how often, the VIP4G will send out PING messages to the Host.

Values (seconds)

300

#### Count

The **Count** field is the maximum number of PING errors such as "Host unreachable" the IPn3G will attempt before the unit will reboot itself to attempt to correct connection issues. If set to zero (0), the unit will never reboot itself.

Values (number)

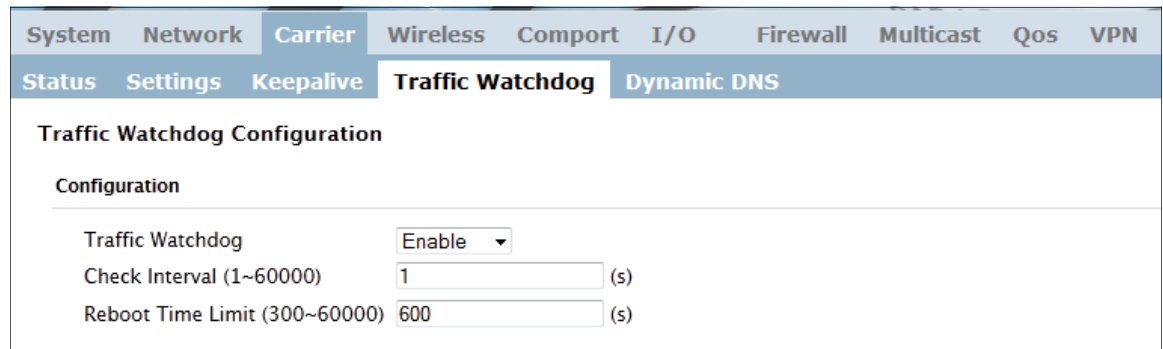
10

## 4.0 Configuration

### 4.3 Carrier

#### 4.3.4 Carrier > Traffic Watchdog

The Wireless Traffic Watchdog will detect if there has been no wireless traffic, or communication with the Cellular carrier for a configurable amount of time. Once that time has elapsed, the unit will reset, and attempt to re-establish communication with the cellular carrier.



System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN
Status	Settings	Keepalive	<b>Traffic Watchdog</b>	Dynamic DNS					

### Traffic Watchdog Configuration

**Configuration**

Traffic Watchdog	Enable	
Check Interval (1~60000)	1	(s)
Reboot Time Limit (300~60000)	600	(s)

Image 4-29: Carrier > Traffic Watchdog

### Traffic Watchdog

Enable or Disable the Traffic Watchdog.

#### Values (Selection)

Enable / Disable

### Check Interval

The Check Interval tells the VIP4G how often (in seconds) to check for wireless traffic to the cellular carrier. (1-60000 seconds)

#### Values (seconds)

1

### Reboot Time Limit

The Reboot Timer will reset the unit if there has been no Cellular RF activity in the configured time. (300 –60000 seconds)

#### Values (seconds)

600



## 4.0 Configuration

### 4.3 Carrier

#### 4.3.5 Carrier > Dynamic DNS

Unless a carrier issues a Static IP address, it may be desirable to use a dynamic DNS service to track dynamic IP changes and automatically update DNS services. This allows the use of a constant resolvable host name for the VIP4G.

The screenshot shows the 'Dynamic DNS' configuration page. At the top, there are tabs for System, Network, Carrier, Wireless, Comport, I/O, Firewall, Multicast, Qos, VPN, and Tools. Under the 'Carrier' tab, there are sub-tabs for Status, Settings, Keepalive, Traffic Watchdog, and Dynamic DNS. The 'Dynamic DNS' sub-tab is selected, showing the 'Dynamic\_DNS Configuration' section. Under 'Configuration', there are fields for DDNS status (set to 'Enable'), Service (set to 'dyndns'), User Name, Password, and Host, each with a corresponding input field.

Image 4-30: Carrier > Traffic Watchdog

#### DDNS Status

This selection allows the use of a Dynamic Domain Name Server (DDNS), for the VIP4G.

##### Values (Selection)

Enable / Disable

#### Service

This is a list of supported Dynamic DNS service providers. Free and premium services are offered, contact the specific providers for more information.

##### Values (selection)

changeip	ods
dyndns	ovh
europyndns	regfish
hn	tzo
noip	zoneedit

#### User Name

Enter a valid user name for the DDNS service selected above.

##### Values (characters)

(none)

#### Password

Enter a valid password for the user name of the DDNS service selected above.

##### Values (characters)

(none)

#### Host

This is the host or domain name for the VIP4G as assigned by the DDNS provider.

##### Values (domain name)

(none)



## 4.0 Configuration

### 4.3 Wireless (WiFi)

#### 4.3.1 Wireless > Status

The Status window gives a summary of all radio or wireless related settings and connections.

The **General Status** section shows the Wireless MAC address of the current radio, the Operating Mode (Access Point, Client, MESH etc), the SSID being used, frequency channel information and the type of security used.

**Traffic Status** shows statistics about the transmitted and received data.

The VIP4G shows information about all Wireless connections in the **Connection Status** section. The Wireless MAC address, Noise Floor, Signal to Noise ratio (SNR), Signal Strength (RSSI), The transmit and receive Client Connection Quality (CCQ), TX and RX data rates, and a graphical representation of the signal level or quality.

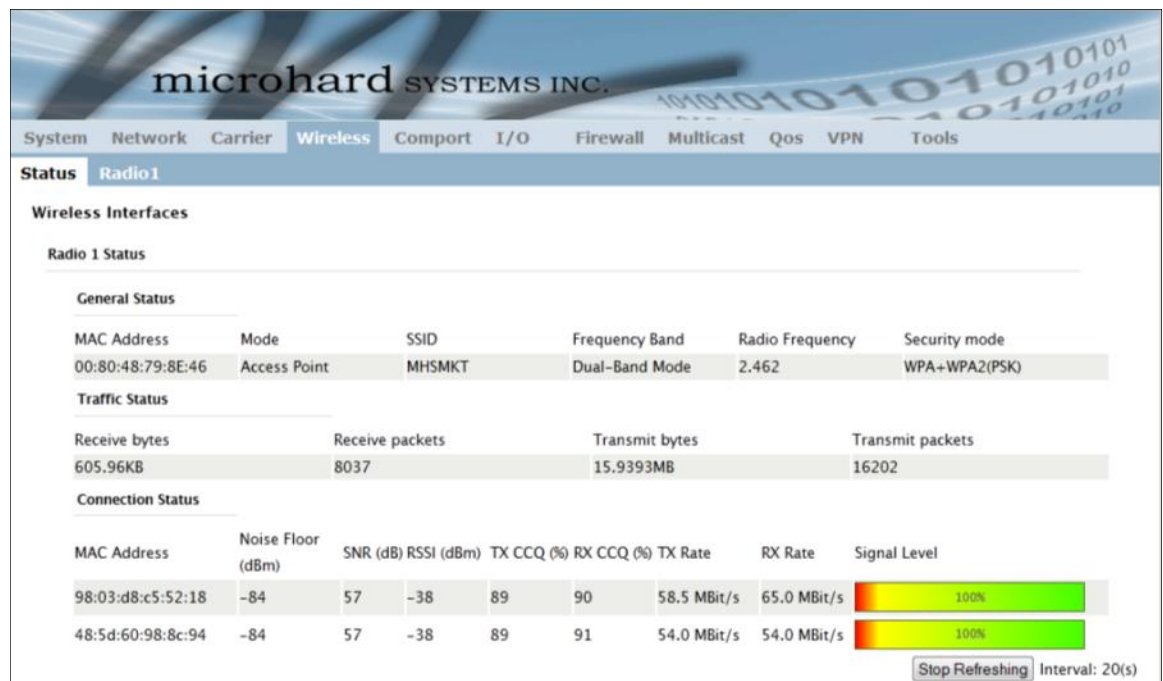


Image 4-31: Wireless > Status

## 4.0 Configuration

### 4.3.2 Wireless > Radio1

#### Radio1 Phy Configuration

The top section of the Wireless Configuration allows for the configuration of the physical radio module. You can turn the radio on or off, and select the channel bandwidth and frequency as seen below.

The screenshot shows the 'Wireless Configuration' window with the 'Radio1' tab selected. The 'Radio1 Phy Configuration' section is expanded, showing various settings for the radio module. The 'Radio' is set to 'On', and the 'Mode' is '802.11NG - High Throughput on 2.4GHz'. Other settings include 'High Throughput Mode' (HT20), 'Advanced Capabilities' (Show), 'MPDU Aggregation' (Enable), 'Short GI' (Enable), 'HT Capabilities Info' (TX-STBC RX-STBC1 DSSS\_CCK-40), 'Maximum AMSDU (byte)' (3839), 'Maximum AMPDU (byte)' (65535), 'Channel-Frequency' (11 - 2.462 GHz), 'Wireless Distance' (10000 m), 'RTS Thr (256~2346)' (OFF), and 'Fragment Thr (256~2346)' (OFF).

Image 4-32: Wireless > Radio Configuration

#### Radio

This option is used to turn the radio module on or off. If turned off Wireless connections can not be made. The default is On.

#### Values (selection)

On / Off

#### Mode

The Mode defines which wireless standard to use for the wireless network. The VIP4G supports all 802.11a/b/g/n modes as seen here. Select the appropriate operating mode from the list.

#### Values (selection)

802.11B ONLY  
802.11BG  
802.11NG-High Throughput 2.4GHz  
802.11A ONLY  
802.11NA-High Throughput 5GHz

The options below are dependant and vary on the operating mode chosen here.

#### Channel BandWidth

Only appears when using 802.11b, bg or a modes. Lower channel bandwidths may provide longer range and be less susceptible to noise but at the trade off of data rates. Higher channel bandwidth may provide greater data rates but will be more susceptible to noise and shorter distance potentials.

#### Values (selection)

20MHz Normal Rate

## 4.0 Configuration

### High Throughput Mode

Select HT20 for a 20MHz channel, or HT40 for a 40 MHz Channel. The 40MHz channel is comprised of 2 adjacent 20MHz channels and the + and—designate to use the higher or lower of the adjacent channels.

#### Values (selection)

**HT20**  
HT40-  
HT40+

#### Advanced Capabilities (Only shown if box is checked)

**MPDU Aggregation** (Enable/Disable) - Allows multiple data frames to be sent in a single transmission block, allowing for acknowledging or retransmitting if errors occur.

**Short GI** (Enable/Disable) - GI (guard interval) is the time the receiver waits for any RF reflections to settle before sampling data. Enabling a short GI (400ns) can increase throughput, but can also increase the error rate in some installations.

HT Capabilities Info - TX-STBC RX-STBC1 DSSS\_CCK-40  
Maximum AMSDU (byte) - 3839  
Maximum AMPDU (byte) - 65535

### Channel-Freq

The Channel-Freq setting allows configuration of which channel to operate on, auto can be chosen where the unit will automatically pick a channel to operate. If a link cannot be established it will try another channel.

#### 2.4 GHz Channels

##### Auto

Channel 01 : 2.412 GHz  
Channel 02 : 2.417 GHz  
Channel 03 : 2.422 GHz  
Channel 04 : 2.427 GHz  
Channel 05 : 2.432 GHz  
Channel 06 : 2.437 GHz  
Channel 07 : 2.442 GHz  
Channel 08 : 2.447 GHz  
Channel 09 : 2.452 GHz  
Channel 10 : 2.457 GHz  
Channel 11 : 2.462 GHz

#### 5 GH Channels

##### Auto

Channel 36: 5.18 GHz  
Channel 40: 5.2 GHz  
Channel 44: 5.22 GHz  
Channel 48: 5.24 GHz  
Channel 149 : 5.745 GHz  
Channel 153 : 5.765 GHz  
Channel 157 : 5.785 GHz  
Channel 161 : 5.805 GHz  
Channel 165 : 5.825 GHz

### Wireless Distance

The Wireless Distance parameter allows a user to set the expected distance the WiFi signal needs to travel. The default is 10km, so the VIP4G will assume that the signal may need to travel up to 10km so it sets various internal timeouts to account for this travel time. Longer distances will require a higher setting, and shorter distances may perform better if the setting is reduced.

#### Values (meters)

**10000**

## 4.0 Configuration

### RTS Thr (256 ~ 2346)

Once the RTS Threshold defined packet size is reached, the system will invoke RTS/CTS flow control. A large RTS Threshold will improve bandwidth, while a smaller RTS Threshold will help the system recover from interference or collisions caused by obstructions.

#### Values (selection)

On / **OFF**

### Fragment Thr (256 ~ 2346)

The Fragmentation Threshold allows the system to change the maximum RF packet size. Increasing the RF packet size reduces the need to break packets into smaller fragments. Increasing the fragmentation threshold slightly may improve performance if a high packet error rate is experienced.

#### Values (selection)

On / **OFF**

### Radio1 Virtual Interface

The bottom section of the Wireless Configuration provides for the configuration of the Mode of the Wireless interface, the TX power, Wireless Network information, and Wireless Encryption.

Radio1 Virtual Interface

Network	LAN
Mode	Access Point
TX bitrate	Auto
Tx Power	17 dbm
WDS	<input checked="" type="radio"/> On <input type="radio"/> Off
ESSID Broadcast	<input checked="" type="radio"/> On <input type="radio"/> Off
SSID	wlan2247
Encryption Type	WPA2 (PSK)
WPA PSK	••••••••
Show password	<input type="checkbox"/>

Image 4-33: Wireless > Radio Configuration

### Network

Choose between LAN or WAN for the Wireless interface. If the unit is configured as a Bridge, only the LAN option will appear in the drop down list.

#### Values (selection)

LAN  
WAN

## 4.0 Configuration

Mode	
There are four available selections for the unit's mode of operation:	<b>Values (selection)</b>
<b>Access Point</b> - An Access Point may provide a wireless data connection to many clients, such as stations, repeaters, or other supported wireless devices such as laptops etc.	Access Point <b>Client</b> Repeater Mesh Point
<b>Station/Client</b> - A Station may sustain one wireless connection, i.e. to an Access Point.	
<b>Repeater</b> - A Repeater can be connected to an Access Point to extend the range and provide a wireless data connection to many clients, such as stations.	
<b>Mesh Point</b> - Units can be configured as a Mesh "Node". When multiple units are configured as a Mesh node, they automatically establish a network between each other. SSID for each radio in a Mesh network must be the same.	

### TX Rate

This setting determines the rate at which the data is to be wirelessly transferred.

The default is 'Auto' and, in this configuration, the unit will transfer data at the highest possible rate in consideration of the receive signal strength (RSSI).

Setting a specific value of transmission rate has the benefit of 'predictability' of that rate, but if the RSSI drops below the required minimum level to support that rate, communications will fail.

802.11 a/b/g	802.11a	802.11n (HT20/HT40)
<b>Auto</b> 1 Mbps (802.11b,g) 2 Mbps (802.11b,g) 5.5 Mbps (802.11b,g) 11 Mbps (802.11b,g) 6 Mbps (802.11a,g) 9 Mbps (802.11a,g) 12 Mbps (802.11a,g) 18 Mbps (802.11a,g) 24 Mbps (802.11a,g) 36 Mbps (802.11a,g) 48 Mbps (802.11a,g) 54 Mbps (802.11a,g)	<b>Auto</b> 6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps	<b>Auto</b> mcs-0 (7.2/15) Mbps mcs-1 (14.4/30.0) Mbps mcs-2 (21.7/45.0) Mbps mcs-3 (28.9/60.0) Mbps mcs-4 (43.3/90.0) Mbps mcs-5 (57.8/120.0) Mbps mcs-6 (65.0/135.0) Mbps mcs-7 (72.2/150.0) Mbps mcs-8 (14.4/30.0) Mbps mcs-9 (28.9/60.0) Mbps mcs-10 (43.3/90.0) Mbps mcs-11 (57.8/120.0) Mbps mcs-12 (86.7/180.0) Mbps mcs-13 (115.6/240.0) Mbps mcs-14 (130.3/270.0) Mbps mcs-15 (144.4/300.0) Mbps

## 4.0 Configuration



Refer to FCC (or as otherwise applicable) regulations to ascertain, and not operate beyond, the maximum allowable transmitter output power and effective isotropic radiated power (EIRP).

This setting establishes the transmit power level which will be presented to the antenna connectors at the rear of the VIP4G. Unless required, the Tx Power should be set not for maximum, but rather for the minimum value required to maintain an adequate system fade margin.

### TX Power

#### Values (selection)

11 dBm	21 dBm
12 dBm	22 dBm
13 dBm	23 dBm
14 dBm	24 dBm
15 dBm	25 dBm
16 dBm	26 dBm
<b>17 dBm</b>	27 dBm
18 dBm	28 dBm
19 dBm	29 dBm
20 dBm	30 dBm



SSID: Service Set Identifier. The 'name' of a wireless network. In an open wireless network, the SSID is broadcast; in a closed system it is not. The SSID must be known by a potential client for it to be able to access the wireless network.

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points. WDS preserves the MAC addresses of client frames across links between access points

### WDS

#### Values (selection)

On / Off

### ESSID Broadcast

Disabling the SSID broadcast helps secure the wireless network. Enabling the broadcast of the SSID (Network Name) will permit others to 'see' the wireless network and perhaps attempt to 'join' it.

#### Values (selection)

On / Off



Change the default value for the Network Name to something unique for your network. Do this for an added measure of security and to differentiate your network from others which may be operating nearby.

All devices connecting to the VIP4G in a given network must use the SSID of the VIP4G. This unique network address is not only a security feature for a particular network, but also allows other networks - with their own unique network address - to operate in the same area without the possibility of undesired data exchange between networks.

### SSID

#### Values (string)

wlan0

### MESH ID

In Mesh Networks, this must be the same for all VIP4G, or VIP Series units participating, similar to the SSID for other wireless networks.

#### Values (string)

(no default)



## 4.0 Configuration



WEP: Wired Equivalency Privacy is a security protocol defined in 802.11b. It is commonly available for Wi-Fi networks and was intended to offer the equivalent security of a wired network, however, it has been found to be not as secure as desired.

Operating at the data link and physical layers, WEP does not provide complete end-to-end security.

Security options are dependent on the version type. This section describes all available options. Export versions may not have all optional available to meet regulatory requirements set government policies.

**WEP:** Wired Equivalency Protocol (WEP) encryption adds some overhead to the data, thereby negatively effecting throughput to some degree.

The image below shows the associated configuration options:

Image 4-34: Encryption Type > WEP

- **Key Generation**  
4 complex WEP keys may be generated based on the supplied Passphrase

**Procedure:** Input a Key Phrase, select the type of Key to be generated using the Generate Key soft button.

Using the same Passphrase on all VIP4G/VIP Series units within the network will generate the same Keys on all units. All units must operate with the same Key selected.

Alternately, key phrases may be entered manually into each Key field.

**WPA:** Wi-Fi Protected Access (WPA/WPA2). It provides stronger security than WEP does. The configuration is essentially the same as for WEP (described above), without the option for automatic Key generation.

### Show Password

Check this box to show the currently configured password for WPA/WPA2 encryption passphrase.

### Values (selection)

unchecked

## 4.0 Configuration

### 4.4 Comport

#### 4.4.1 Comport > Status

The Status window gives a summary of the Serial port on the VIP4G. The Status window shows if the com port has been enabled, how it is configured (Connect As), and the connection status.

The screenshot displays the web interface of the microhard SYSTEMS INC. VIP4G device. The top navigation bar includes tabs for System, Network, Carrier, Wireless, Comport, I/O, Firewall, Multicast, Qos, VPN, and Tools. The 'Comport' tab is selected, and the 'Status' sub-tab is active. The 'Comport Status' section is titled 'Port Status' and contains two main areas: 'General Status' and 'Traffic Status'.

General Status			
Port Status	Baud Rate	Connect As	Connect Status
Enable	9600	TCP Server	Not Active

Traffic Status			
Receive bytes	Receive packets	Transmit bytes	Transmit packets
0	0	0	0

At the bottom right of the Traffic Status section, there is a 'Stop Refreshing' button and a text label 'Interval: 20 (in seconds)'.

Image 4-35: Comport > Comport Status

## 4.0 Configuration

### 4.4 Comport

#### 4.4.2 Comport > Settings

This menu option is used to configure the serial device server for the serial communications port. Serial device data may be brought into the IP network through TCP, UDP, or multicast; it may also exit the VIP4G network on another VIP Series' serial port. The fully-featured RS232 interface supports hardware handshaking.

The screenshot displays the 'Comport' configuration page of the microhard SYSTEMS INC. VIP4G web interface. The top navigation bar includes links for System, Network, Carrier, Wireless, Comport (selected), I/O, Firewall, Multicast, Qos, VPN, and Tools. Below this, the 'Status' and 'Settings' tabs are visible, with 'Settings' being the active tab. The main content area is titled 'Comport Configuration' and contains two sections: 'Comport Configuration' and 'TCP Configuration'. The 'Comport Configuration' section includes settings for Com Port status (Enable), Channel Mode (RS232), Data Baud Rate (9600), Data Format (8N1), Flow Control (none), Pre-Data Delay (ms) (100), Post-Data Delay (ms) (100), Data Mode (Seamless and Transparent radio buttons, with Transparent selected), Character Timeout (0), Maximum Packet Size (1024), Priority (Normal, Medium, and High radio buttons, with Normal selected), No-Connection Data (Disable and Enable radio buttons, with Enable selected), TCP MODBUS Status (Disable and Enable radio buttons, with Disable selected), and IP Protocol Config (TCP Server). The 'TCP Configuration' section includes Local Listening port (20001) and Incoming Connection Timeout (300).

Comport Configuration	
Com Port status	Enable
Channel Mode	RS232
Data Baud Rate	9600
Data Format	8N1
Flow Control	none
Pre-Data Delay (ms)	100
Post-Data Delay (ms)	100
Data Mode	<input type="radio"/> Seamless <input checked="" type="radio"/> Transparent
Character Timeout	0
Maximum Packet Size	1024
Priority	<input checked="" type="radio"/> Normal <input type="radio"/> Medium <input type="radio"/> High
No-Connection Data	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
TCP MODBUS Status	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IP Protocol Config	TCP Server
TCP Configuration	
Local Listening port	20001
Incoming Connection Timeout	300

Image 4-36: Comport > Settings Configuration

## 4.0 Configuration

### Com1 Port Status

Select operational status of the Com1 Serial Port. The port is disabled by default.

#### Values (selection)

**Disabled** / Enable

### Channel Mode

Determines which serial interface shall be used to connect to external devices: RS232, RS485, or RS422. When an interface other than RS232 is selected, the DE9 port will be inactive.

#### Values (selection)

**RS232**  
RS485  
RS422

### Data Baud Rate

The serial baud rate is the rate at which the modem is to communicate with the attached local asynchronous device.

#### Values (bps)

921600	<b>9600</b>
460800	7200
230400	4800
115200	3600
57600	2400
38400	1200
28800	600
19200	300
14400	



Note: Most PCs do not readily support serial communications greater than 115200bps.

### Data Format

This setting determines the format of the data on the serial port. The default is 8 data bits, No parity, and 1 Stop bit.

#### Values (selection)

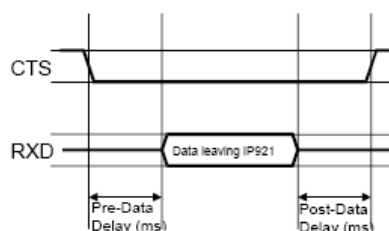
<b>8N1</b>	7N2
8N2	7E1
8E1	7O1
8O1	7E2
7N1	7O2



Software flow control (XON/XOFF) is not supported.

### Flow Control

Flow control may be used to enhance the reliability of serial data communications, particularly at higher baud rates. If the attached device does not support hardware handshaking, leave this setting at the default value of 'None'. When CTS Framing is selected, the VIP4G uses the CTS signal to gate the output data on the serial port.



#### Values (selection)

**None**  
Hardware  
CTS Framing

Drawing 4A: CTS Output Data Framing

## 4.0 Configuration

### Pre-Data Delay

Refer to **Drawing 6A** on the preceding page.

Values (time (ms) )

100

### Post-Data Delay

Refer to **Drawing 6A** on the preceding page.

Values (time (ms) )

100

### Date Mode

This setting defines the serial output data framing. In Transparent mode (default), the received data will be output promptly from the VIP4G.

Values (selection)

Seamless / **Transparent**

When set to Seamless, the serial port server will add a gap between data frames to comply with the MODBUS protocol for example. See 'Character Timeout' below for related information.

### Character Timeout

In Seamless mode (see Data Mode described on the preceding page), this setting determines when the serial server will consider the recently-received incoming data as being ready to transmit. As per the MODBUS standard, frames will be marked as 'bad' if the time gap between frames is greater than 1.5 characters, but less than the Character Timeout value.

Values (characters)

0

The serial server also uses this parameter to determine the time gap inserted between frames. It is measured in 'characters' and related to baud rate.

Example: If the baud rate is 9600bps, it takes approximately 1ms to move one character. With the Character Timeout set to 4, the timeout period is 4ms. When the calculated time is less than 3.5ms, the serial server will set the character timeout to a minimum value of 3.5ms.

If the baud rate is greater than 19200bps, the minimum character timeout is internally set to 750us (microseconds).

### Maximum Packet Size

Defines the buffer size that the serial server will use to receive data from the serial port. When the server detects that the Character Timeout criteria has been met, or the buffer is full, it packetizes the received frame and transmits it.

Values (bytes)

1024

### Priority

This setting effects the quality of service associated with the data traffic on the COM port.

Values (selection)

**Normal** / Medium / High

## 4.0 Configuration

### No-Connection Data

When enabled the data will continue to buffer received on the serial data port when the radio loses synchronization. When disabled the VIP4G will disregard any data received on the serial data port when radio synchronization is lost.

#### Values (selection)

**Disable** / Enable

### MODBUS TCP Status

This option will enable or disable the MODBUS decoding and encoding features.

#### Values (selection)

**Disable** / Enable

### MODBUS TCP Protection

The field allows the MODBUS TCP Protection Status flag to be enabled or disabled. If enabled the MODBUS data will be encrypted with the MODBUS Protection Key.

#### Values (selection)

**Disable** / Enable

### MODBUS TCP Protection Key

MODBUS encryption key used for the MODBUS TCP Protection Status feature.

#### Values (string)

1234



## 4.0 Configuration



The protocol selected in the IP Protocol Config field will determine which configuration options appear in the remainder of the COM1 Configuration Menu.

### IP Protocol Config

#### Values (selection)

TCP Client  
 TCP Server  
 TCP Client/Server  
 UDP Point-to-Point  
 UDP Point-to-Multipoint (P)  
**UDP Point-to-Multipoint(MP)**  
 UDP Multipoint-to-Multipoint  
 SMTP Client  
 C12.22

This setting determines which protocol the serial server will use to transmit serial port data over the VIP4G network.

The protocol selected in the IP Protocol Config field will determine which configuration options appear in the remainder of the COM1 Configuration Menu.

**TCP Client:** When TCP Client is selected and data is received on its serial port, the VIP4G takes the initiative to find and connect to a remote TCP server. The TCP session is terminated by this same unit when the data exchange session is completed and the connection timeout has expired. If a TCP connection cannot be established, the serial port data is discarded.



UDP: User Datagram Protocol does not provide sequencing information for the packets sent nor does it establish a 'connection' ('handshaking') and is therefore most suited to communicating small packets of data.

- **Remote Server Address**  
 IP address of a TCP server which is ready to accept serial port data through a TCP connection. For example, this server may reside on a LAN network server.  
 Default: **0.0.0.0**
- **Remote Server Port**  
 A TCP port which the remote server listens to, awaiting a session connection request from the TCP Client. Once the session is established, the serial port data is communicated from the Client to the Server.  
 Default: **20001**
- **Outgoing Connection Timeout**  
 This parameter determines when the VIP4G will terminate the TCP connection if the connection is in an idle state (i.e. no data traffic on the serial port).  
 Default: **60** (seconds)



TCP: Transmission Control Protocol in contrast to UDP does provide sequencing information and is connection-oriented; a more reliable protocol, particularly when large amounts of data are being communicated.

Requires more bandwidth than UDP.

**TCP Server:** In this mode, the VIP4G Series will not INITIATE a session, rather, it will wait for a Client to request a session of it (it's being the Server—it 'serves' a Client). The unit will 'listen' on a specific TCP port. If a session is established, data will flow from the Client to the Server, and, if present, from the Server to the Client. If a session is not established, both Client-side serial data, and Server-side serial data, if present, will be discarded.

- **Local Listening Port**  
 The TCP port which the Server listens to. It allows a TCP connection to be created by a TCP Client to carry serial port data.  
 Default: **20001**
- **Incoming Connection Timeout**  
 Established when the TCP Server will terminate the TCP connection is the connection is in an idle state.  
 Default: **300** (seconds)

## 4.0 Configuration

### IP Protocol Config (Continued...)



A UDP or TCP port is an application end-point. The IP address identifies the device and, as an extension of the IP address, the port essentially 'fine tunes' where the data is to go 'within the device'.

Be careful to select a port number that is not predetermined to be associated with another application type, e.g. HTTP uses port 80.



Multicast is a one-to-many transmission of data over an IP network. It is an efficient method of transmitting the same data to many recipients. The recipients must be members of the specific multicast group.



TTL: Time to Live is the number of hops a packet can travel before being discarded.

In the context of multicast, a TTL value of 1 restricts the range of the packet to the same subnet.

**TCP Client/Server:** In this mode, the VIP4G will be a combined TCP Client and Server, meaning that it can both initiate and serve TCP connection (session) requests. Refer to the TCP Client and TCP Server descriptions and settings described previously as all information, combined, is applicable to this mode.

**UDP Point-to-Point:** In this configuration the VIP4G will send serial data to a specifically-defined point, using UDP packets. This same VIP4G will accept UDP packets from that same point.

- **Remote IP Address**  
IP address of distant device to which UDP packets are sent when data received at serial port.  
Default: **0.0.0.0**
- **Remote Port**  
UDP port of distant device mentioned above.  
Default: **20001**
- **Listening Port**  
UDP port which the IP Series listens to (monitors). UDP packets received on this port are forwarded to the unit's serial port.  
Default: **20001**

**UDP Point-to-Multipoint (P):** This mode is configured on an VIP4G which is to send multicast UDP packets; typically, the Access Point in the VIP4G network.

- **Multicast IP Address**  
A valid multicast address this unit uses to send multicast UDP packets upon receiving data from the serial port. The default value is a good example of a valid multicast address.  
Default: **224.1.1.1**
- **Multicast Port**  
A UDP port that this IP Series will send UDP packets to. The Multipoint (MP - see the UDP Point-to-Multipoint (MP) description) stations should be configured to listen to this point in order to receive multicast packets from this VIP4G unit.  
Default: **20001**
- **Listening Port**  
The UDP port that this unit receives incoming data on from multiple remote units.  
Default: **20011**
- **Time to Live**  
Time to live for the multicast packets.  
Default: **1** (hop)

## 4.0 Configuration

### IP Protocol Config (Continued...)



In a Point-to-Multipoint (PMP) network topology which is to utilize UDP multicast, typically the MASTER would be configured as 'P' (the POINT) and the REMOTES would be configured as '(MP)' (the MULTIPOINTS).

**UDP Point-to-Multipoint (MP):** This protocol is selected on the units which are to receive multicast UDP packets, typically the Remote units. See the previous description of UDP Point-to-Multipoint (P).

- **Remote IP Address**  
The IP address of a distant device (VIP4G or, for example, a PC) to which the unit sends UDP packets of data received on the serial port. Most often this is the IP address of the Access Point.  
Default: **0.0.0.0**
- **Remote Port**  
The UDP port associated with the Remote IP Address (above). In the case of this 'Remote' being the VIP Series Station, the value in this field should match the Listening Port of the Access Point (see UDP Point-to-Multipoint (P)).  
Default: **20011**
- **Multicast IP Address**  
A valid MULTICAST address that this unit will use to receive multicast UDP packets sent by a UDP Point-to-Multipoint (P) unit. Note that the default value for this field matches the default Multicast IP Address of the UDP Point-to-Multipoint (P) configuration described on the previous page.  
Default: **224.1.1.1**
- **Multicast Port**  
The UDP port that this unit will use, along with the Multicast IP Address detailed above, to receive the multicast UDP packets sent by the UDP Point-to-Multipoint (P) unit.  
Default: **20001**

#### UDP Multipoint-to-Multipoint

- **Multicast IP Address**  
A valid multicast address the unit will use to send multicast UDP packets upon receiving them at its serial port.  
Default: **224.1.1.1**
- **Multicast Port**  
UDP port that the packets are sent to. Multipoint stations should be configured to listen to this port in order to receive multicast packets.  
Default: **20011**
- **Time to Live**  
Time to live for the multicast packets.  
Default: **1** (hop)
- **Listening Multicast IP Address**  
A valid multicast address the unit is to listen to receive multicast UDP packets sent by another UDP Multipoint-to-Multipoint unit.  
Default: **224.1.1.1**
- **Listening Multicast Port**  
UDP port that the unit will listen to for multicast UDP packets sent by another UDP Multipoint-to-Multipoint unit.  
Default: **20011**

## 4.0 Configuration

### IP Protocol Config (Continued...)

**SMTP Client:** If the VIP4G has Internet access, this protocol may be used to send the data received on the serial port (COM1), in a selectable format (see Transfer Mode (below)), to an e-mail addressee. Both the SMTP Server and the e-mail addressee must be 'reachable' for this feature to function.



SMTP: Simple Mail Transport Protocol is a protocol used to transfer mail across an IP network.

- **Mail Subject**  
Enter a suitable 'e-mail subject' (e-mail heading).  
Default: **COM1 Message**
- **Mail Server (IP/Name)**  
IP address or 'Name' of SMTP (Mail) Server.  
Default: **0.0.0.0**
- **Mail Recipient**  
A valid e-mail address for the intended addressee, entered in the proper format.  
Default: **host@**
- **Message Max Size**  
Maximum size for the e-mail message.  
Default: **1024**
- **Timeout (s)**  
How long the unit will wait to gather data from the serial port before sending an e-mail message; data will be sent immediately upon reaching Message Max Size.  
  
Default: **10**
- **Transfer Mode**  
Select how the data received on COM1 is to be sent to the email addressee.  
Options are: Text, Attached File, Hex Code.  
Default: **Text**

## 4.0 Configuration

### 4.5 I/O

#### 4.5.1 I/O > Status

##### I/O Status

The VIP4G has 4 status inputs, which can be used with various alarms and sensors for monitoring, telling the modem when certain events have occurred, such as an intrusion alarm on a door, a temperature threshold has been exceeded, or a generator has failed, out of fuel. Also included are 4 outputs, that can be used to drive external relays to remotely control equipment and devices.

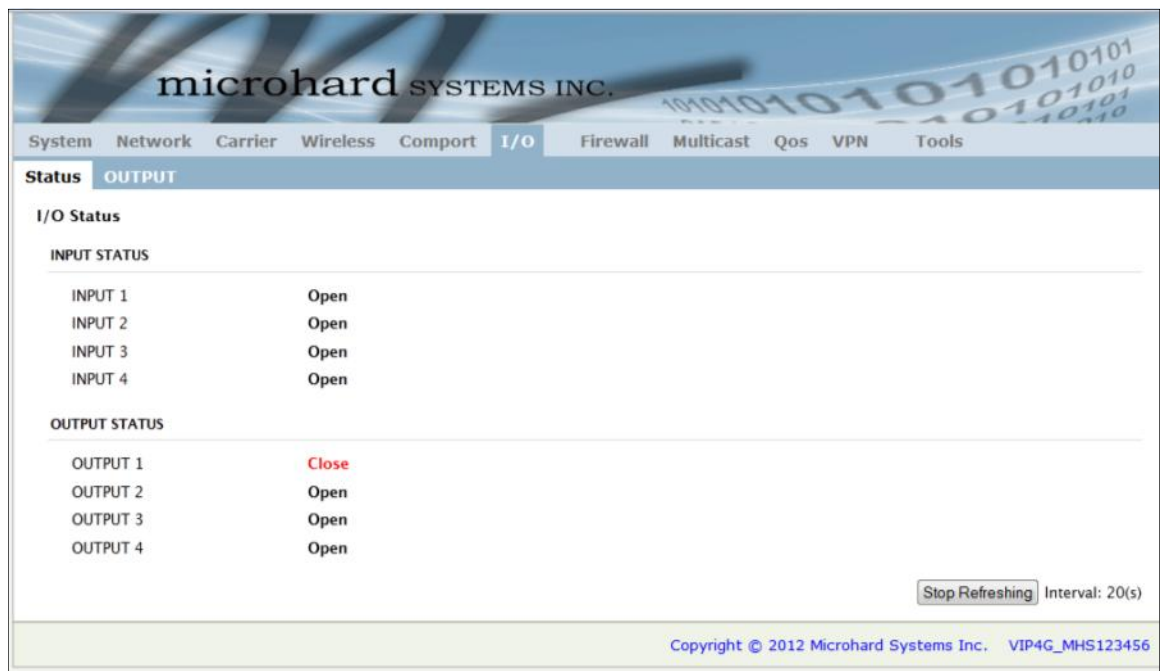


Image 4-37: I/O > Status

##### Input Status

The WebUI will display the current state of each input. The I/O pins are all normally open so an open status indicates that there is nothing connected to the input pins, or that an event has not occurred to trigger the input.

##### Output Status

The WebUI will display the current state of each control output. Using the Output menu discussed in the next section, a user can remotely control the status of the output pins.

## 4.0 Configuration

### 4.5 I/O

#### 4.5.2 I/O > OUTPUT

##### OUTPUT Configuration

Each of the 4 Outputs can be controlled separately, allowing a user to remotely trigger an event.



Image 4-38: I/O > OUTPUT



## 4.0 Configuration

### 4.6 Firewall

#### 4.6.1 Firewall > Status

Firewall Status allows a user to see detailed information about how the firewall is operating. The All, Filter, Nat, Raw, and Mangle options can be used to view different aspects of the firewall.

**microhard SYSTEMS INC.**

System Network Carrier Wireless Comport I/O **Firewall** Multicast Qos VPN Tools

**Status** General Rules Port Forwarding MAC-IP List

**Firewall Status**

Display Status and Rules of Firewall All Check

Target Filter

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options
1	4306	831K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
2	7	690	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
3	216	11232	syn_flood	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02
4	2146	160K	input_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
5	2146	160K	input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain FORWARD (policy DROP 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options
1	72067	45M	zone_wan2_MSSFIX	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
2	72067	45M	zone_wan_MSSFIX	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
3	70623	45M	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
4	1444	77867	forwarding_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
5	1444	77867	forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
6	0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options
1	4058	3772K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
2	7	690	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0	
3	1992	140K	output_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
4	1991	140K	output	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Image 4-39: Firewall > Status

## 4.0 Configuration

### 4.6.2 Firewall > General

The General Firewall settings allow users to enable or disable the firewall, and to decide which areas of the modem to protect. The Firewall can also be reset to factory defaults from this area of the WebUI.

Image 4-40: Firewall > General

#### Firewall Status

When enabled, the firewall settings are in effect. When disabled, none of the settings configured in the menu's below have an effect, the modem is "open".

##### Values

Disable / Enable

#### WAN Remote Management

Allow remote management of the VIP4G on the WAN side using the WebUI on port 80(HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN (or 4G if enabled)..

##### Values

Disable / **Enable**

#### 4G Remote Management

Allow remote management of the VIP4G from the 4G side of using the WebUI on port 80(HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN (or WAN if enabled)..

##### Values

Disable / **Enable**

## 4.0 Configuration

### WAN Request

When Blocked the VIPn4G will block all requests from devices on the WAN unless specified otherwise in the Access Rules, MAC List, IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the **WAN Remote Management** option.

#### Values

Block / **Allow**

### 4G Request

When Blocked all requests from devices on the 4G (Wireless Carrier) side will be blocked, unless specified otherwise in the Access Rules, MAC List, IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the **4G Remote Management** option.

#### Values

Block / **Allow**

### LAN to WAN Access Control

Allows or Blocks traffic from the LAN accessing the WAN unless specified otherwise using the Access Rules, MAC, and IP List configuration.

#### Values

Block / **Allow**

### LAN to 4G Access Control

Allows or Blocks traffic from the LAN accessing the 4G connection unless specified otherwise using the Access Rules, MAC, and IP List configuration.

#### Values

Block / **Allow**

### WAN to LAN Access Control

Allows or Blocks traffic from the WAN accessing the devices on the LAN connections unless specified otherwise using the Access Rules, MAC, and IP List configuration.

#### Values

Block / **Allow**

### 4G to LAN Access Control

Allows or Blocks traffic from the 4G accessing the devices on the LAN connections unless specified otherwise using the Access Rules, MAC, and IP List configuration.

#### Values

Block / **Allow**

## 4.0 Configuration

### 4.6.3 Firewall > Rules

Once the firewall is turned on, rules configuration can be used to define specific rules on how local and remote devices access different ports and services. MAC List and IP List are used for general access, and are applied before rules are processed.

Name	Action	Source	Source IP	Destination	Destination IP	Destination Port	Protocol
rule1	Accept	None	192.168.0.0/255.255.255	None	192.168.0.0/255.255.255	0	TCP

Image 4-41: Firewall > Rules

#### Rule Name

The rule name is used to identify the created rule. Each rule must have a unique name and up to 10 characters can be used.

#### Values (10 Chars)

characters

#### Action

The Action is used to define how the rule handles the connection request.

#### Values (selection)

ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.

ACCEPT  
DROP  
REJECT

This is configured based on how the **WAN/4G Request** and **LAN to WAN/4G Access Control** are configured in the previous menus.

#### Source

Select the zone which is to be the source of the data traffic. WAN applies to the WAN RJ45 connection, and 4G refers to the connection to the cellular carrier. The LAN refers to local connections on the VIP4G (Ethernet/WiFi).

#### Values

LAN  
WAN  
4G  
**None**

## 4.0 Configuration

### Source IP

If a valid IP/Network address is specified, the action will apply against that address; otherwise, leaving the default value of 0.0.0.0/0 in this field results in the action applying to all source IP addresses.

#### Values (IP Address)

192.168.0.0/255.255.255.0

### Destination Zone

Select the zone which is the intended destination of the data traffic. WAN applies to the wireless connection to the cellular carrier and the LAN refers to local connections on the IPn3G (Ethernet/WiFi)

#### Values (selection)

LAN  
WAN  
4G  
None

### Destination IP

If a valid IP/Network address is specified, the action will apply against that address; otherwise, leaving the default value of 0.0.0.0/0 in this field results in the action applying to all source IP addresses.

#### Values (IP Address)

192.168.0.0/255.255.255.0

### Destination Port

This field is used to define a port or service used in the rule (i.e. Port 80 = HTTP which is generally a web server)

#### Values (port)

0

### Protocol

The protocol field defines the transport protocol type controlled by the rule.

#### Values

TCP  
UDP  
ICMP  
all

## 4.0 Configuration

### 4.6.4 Firewall > Port Forwarding

Port forwarding can be used to forward traffic coming in from the 4G and/or WAN to a specific IP Address and Port on the LAN. Port forwarding can be used in combination with other firewall features, but the Firewall must be enabled for Port forwarding to be in effect.

Image 4-42: Firewall > Port Forwarding

#### DMZ Mode

Enable or disable DMZ Mode. DMZ can be used to forward all traffic to the DMZ Server IP listed below.

#### Values (selection)

**Disable** / Enable

#### DMZ Source

Select the source for the DMZ traffic, either 4G or from WAN.

#### Values (selection)

**4G** / WAN

#### DMZ Server IP

Enter the IP address of the DMZ server on the LAN side of the VIP4G.

#### Values (IP Address)

**192.168.100.100**

#### Exception Port

Enter a exception port number that will NOT be forwarded to the DMZ server IP. Usually a configuration or remote management port that is excluded to retain external control of the VIP4G.

#### Values (Port #)

**443**



## 4.0 Configuration

Name	
This is simply a field where a convenient reference or description is added to the rule. Each Forward must have a unique rule name and can use up to 10 characters.	<div>Values (10 chars)</div> <div>Forward</div>
Source	
Select the source for the DMZ traffic, either 4G or from WAN.	<div>Values (selection)</div> <div>4G / WAN</div>
Internal Server IP	
Enter the IP address of the intended internal (i.e. on LAN side of VIP4G) server. This is the IP address of the device you are forwarding traffic to.	<div>Values (IP Address)</div> <div>192.168.2.1</div>
Internal Port	
Target port number of internal server on the LAN IP entered above.	<div>Values (Port #)</div> <div>3000</div>
Protocol	
Select the type of transport protocol used. For example Telnet uses TCP, SNMP uses UDP, etc.	<div>Values</div> <div>TCP UDP Both</div>
External Port	
Port number of incoming request (from 4G/WAN-side).	<div>Values (Port #)</div> <div>2000</div>

## 4.0 Configuration

### 4.6.5 Firewall > MAC-IP List

MAC List configuration can be used to control which physical LAN devices can access the ports on the VIP4G, by restricting or allowing connections based on the MAC address. IP List configuration can be used to define who or what can access the VIP4G, by restricting or allowing connections based on the IP Address/Subnet.

MAC-IP List can be used alone or in combination with LAN to WAN/4G Access Control to provide secure access to the physical ports of the VIP4G.

**Firewall MAC/IP List**

**Firewall MAC List Configuration**

Name:

Action:

Mac Address:

**Firewall IP List Configuration**

Name:

Action:

Source:

Source IP:

Destination IP:

**Firewall MAC List Summary**

Name	Action	Mac Address
------	--------	-------------

**Firewall IP List Summary**

Name	Action	Source	Source IP	Destination IP
------	--------	--------	-----------	----------------

Image 4-43: Firewall > MAC-IP List

### Firewall MAC List Configuration

The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.

#### Rule Name

Values (10 chars)

MAC\_List

Specify the MAC Address to be added to the list. Must be entered in the correct format as seen above. Not case sensitive.

#### MAC Address

Values (MAC Address)

00:00:00:00:00:00

## 4.0 Configuration

### Firewall MAC List Configuration (Continued)

Action	
<p>The Action is used to define how the rule handles the connection request.</p> <p>ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.</p>	<p><b>Values (selection)</b></p> <p><b>ACCEPT</b> DROP REJECT</p>

### Firewall IP List Configuration

Rule Name	
The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.	<div>Values (10 chars)</div> <div>IP_List</div>
Action	
The Action is used to define how the rule handles the connection request. ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.	<div>Values (selection)</div> <div>ACCEPT / DROP / REJECT</div>
Source	
Enter the specific zone that the IP List will apply to, 4G (Cellular), WAN , LAN (Ethernet, WiFi) or None (both).	<div>Values (Selection)</div> <div>LAN / WAN/ 4G / NONE</div>
Source Address	
Specify the specific IP or Network address (With /subnet, for example 192.168.0.0/24 will apply to all IP addresses in the 192.168.0.1 - 192.168.0.254 range (subnet /24 = 255.255.255.0).	<div>Values (IP Address)</div> <div>0.0.0.0/0</div>
Destination Address	
Optional, enter a destination IP address to make the IP list more specific. Leave as 0.0.0.0/0 to not use.	<div>Values (IP Address)</div> <div>0.0.0.0/0</div>

## 4.0 Configuration

### 4.7 Multicast

#### Multicast Configuration

Multicast can be enabled or disabled for the VIP4G. This section allows for the configuration of the Multicast feature.

Multicast Configuration Summary					
Name	Local IP	Remote IP	Source IP	Source Mask	Group IP
4	192.168.2.1	192.168.5.1	192.168.2.200	255.255.255.0	239.255.255.200

Image 4-44: Multicast

#### Mode

Enable or Disable Multicast in the VIP4G

Values (selection)

Disable / Enable

#### Rate

Use the drop down selection to chose the Multicast rate.

Values (selection)

6	24
9	36
12	<b>48</b>
18	54

## 4.0 Configuration

Name	
Provide a name for the Multicast configuration. Used as reference.	Values (characters) Disable / Enable
Local IP	
Local LAN IP Address of the VIP4G interface connected to the Multicast Device/Source.	Values (IP Address) 192.168.2.1
Remote IP	
IP Address of the remote LAN IP of the VIP4G/VIP Series in which to send the multicast data.	Values (IP Address) 192.168.5.1
Source IP	
IP Address of the Multicast PC/Device.	Values (IP Address) 192.168.2.200
Source Mask	
Subnet Mask of the Multicast PC/Device.	Values (IP Address) 255.255.255.0
Group IP	
The Multicast group IP Address. Destination must also be part of the Multicast group.	Values (IP Address) 239.255.255.200

## 4.0 Configuration

### 4.8 QoS

#### 4.8.1 QoS > Status

QoS Status gives a visual overview of the QoS configuration as seen below.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
Status	Class	Local	Interface							
Quality of Service Statistics										
LAN Port Status										
General Status										
Target	Rate			Ceil			Burst			
High	1000bit			1000bit			128b			
Medium_high	2000Kbit			3000Kbit			128b			
Medium	20000Kbit			20000Kbit			380b			
Medium_low	1000bit			1000bit			128b			
low	1000bit			1000bit			128b			
Traffic Status										
Target	Sent (bytes)			Sent (pkts)			Rate (bit)			
High	0			0			0bit			
Medium_high	0			0			0bit			
Medium	42			1			24bit			
Medium_low	0			0			0bit			
low	0			0			0bit			
WAN Port Status										
General Status										
Target	Rate			Ceil			Burst			
High	1000bit			1000bit			128b			
Medium_high	2000Kbit			3000Kbit			256b			
Medium	20000Kbit			20000Kbit			252b			
Medium_low	1000bit			1000bit			128b			
low	1000bit			1000bit			128b			
Traffic Status										
Target	Sent (bytes)			Sent (pkts)			Rate (bit)			
High	0			0			0bit			
Medium_high	0			0			0bit			
Medium	403			1			200bit			
Medium_low	0			0			0bit			
low	0			0			0bit			

Image 4-45: QoS > Status



## 4.0 Configuration

### 4.8.2 QoS > Class

The QoS class menu allows a user to enable or disable the QoS service. In addition, it is possible to fine tune the different class rates, ceiling, and burst limits for each class.

**Qos Class Configuration**

**Qos Mode**

Qos Mode: Enable

**LAN Port Qos Class Configuration**

Target	Rate	Ceil	Burst
High	1 kbit	1 kbit	1 kbit
Medium_high	2 Mbit	3 Mbit	1 kbit
Medium	20 Mbit	20 Mbit	3 kbit
Medium_low	1 kbit	1 kbit	1 kbit
Low	1 kbit	1 kbit	1 kbit

**WAN Port Qos Class Configuration**

Target	Rate	Ceil	Burst
High	1 kbit	1 kbit	1 kbit
Medium_high	2 Mbit	3 Mbit	2 kbit
Medium	20 Mbit	20 Mbit	2 kbit
Medium_low	1 kbit	1 kbit	1 kbit
Low	1 kbit	1 kbit	1 kbit

Image 4-46: QoS > Class

#### QoS Mode

Use this option to enable or disable the QoS features of the VIP4G. By default QoS is not enabled.

Values (selection)

Enable / Disable

## 4.0 Configuration

### 4.8.3 QoS > Local

This tab is used to actually assign data to a QoS class. You can customize the QoS rules to match the desired operation.

The screenshot displays the 'Qos Local Configuration' page. The 'Interface' dropdown is set to 'LAN', 'Target' to 'High', 'Protocol' to 'TCP'. There are empty input fields for 'Source IP', 'Destination IP', 'Destination Port', and 'Ports'. An 'Add Local rule' button is located below the input fields. The 'Qos Local Summary' table at the bottom has the following structure:

Interface	Target	Source IP	Destination IP	Protocol	Destination Port	Ports
-----------	--------	-----------	----------------	----------	------------------	-------

Image 4-47: QoS > Local

#### Interface

Select the interface (LAN / WAN / 4G) in which the QoS applies.

Values (selection)

LAN / WAN / 4G

#### Target

Select the target class for the QoS rule, the class specifics can be modified in the Class menu.

Values (selection)

High  
Medium\_high  
Medium  
Medium\_low  
Low

#### Source IP

Enter the source IP.

Values (IP Address)

(IP Address)

## 4.0 Configuration

### Destination IP

Enter the destination IP Address.

Values (IP Address)

*(IP Address)*

### Protocol

Select the protocol type, TCP, UDP or ICMP.

Values (selection)

TCP  
UDP  
ICMP

### Destination Port

Enter the port number for the destination.

Values (port#)

*port #*

### Ports

Enter the port number.

Values (port#)

*port #*

## 4.0 Configuration

### 4.8.4 QoS > Interface

This tab is used to configure the LAN, WAN and 4G interfaces for QoS.

The screenshot shows the 'QoS > Interface' configuration page. It has a top navigation bar with tabs: System, Network, Carrier, Wireless, Comport, I/O, Firewall, Multicast, Qos, VPN, and Tools. Below this is a sub-navigation bar with tabs: Status, Class, Local, and Interface (which is selected). The main content area is titled 'Qos Interface Configuration' and contains three sections: 'Qos Interface wan Configuration', 'Qos Interface wan2 Configuration', and 'Qos Interface lan Configuration'. Each section has three fields: 'Interface Mode' (a dropdown menu with 'Enable' selected), 'Target' (a dropdown menu with 'Medium' selected), and 'Bandwidth (Mbit)' (a text input field with '20' entered).

Image 6-48: QoS > Interface

#### QoS Interface LAN / WAN / 4G Configuration.

##### Interface Mode

Enable or Disable QoS on the selected interface.

Values (selection)

Enable / Disable

##### Target

Select the target class for the QoS rule, the class specifics can be modified in the Class menu.

Values (selection)

High  
Medium\_high  
**Medium**  
Medium\_low  
Low

##### Bandwidth

Enter the Bandwidth.

Values (Mbit)

20

## 4.0 Configuration

### 4.9 VPN

#### 4.9.1 VPN > Summary

A Virtual Private Network (VPN) may be configured to enable a tunnel between the VIP4G and a remote network.. The VIP4G supports VPN IPsec Gateway to Gateway (site-to-site) tunneling, meaning you are using the VIP4G to connect a tunnel to network with VPN capabilities. The IPn3G can also operate as a L2TP Server, allowing users to VPN into the unit from a remote PC, and a L2TP Client.

microhard SYSTEMS INC.

System Network Carrier Wireless Comport I/O Firewall Multicast Qos **VPN** Tools

**Summary** Gateway To Gateway Client To Gateway VPN Client Access L2TP Server

**Summary**

**Gateway To Gateway**

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
<a href="#">Add</a>								

**Client To Gateway**

No.	Name	Status	IP Address	Remote Server Gateway	Tunnel Test	Config.
<a href="#">Add</a>						

**L2TP Server**

Status	Local IP	Client IP Range Start	Client IP Range End	Server Test	Config.
disable				N/A	<a href="#">Edit</a>

**L2TP Connection List**

No.	Remote Address	L2TP IP Address	Start Time	Duration	RX Bytes	TX Bytes
-----	----------------	-----------------	------------	----------	----------	----------

**VPN Client Access**

No.	Username	Config.
<a href="#">Add</a>		

[Stop Refreshing](#) Interval: 20

Image 4-49: VPN > Summary

## 4.0 Configuration

### 4.9.2 VPN > Gateway To Gateway (Site-to-Site)

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
<div>Summary Gateway To Gateway Client To Gateway VPN Client Access L2TP Server</div> <div> <h4>Gateway To Gateway</h4> <div>Add a New Tunnel</div> <div> <div>Tunnel Name</div> <div>Enable <input checked="" type="checkbox"/></div> </div> <div> <h4>Local Group Setup</h4> <div> <div>Gateway IP Address</div> <div>Group Subnet IP</div> <div>Group Subnet Mask</div> <div>Group Server IP</div> </div> </div> <div> <h4>Remote Group Setup</h4> <div> <div>Gateway IP Address</div> <div>Server ID</div> <div>Group Subnet IP</div> <div>Group Subnet Mask</div> </div> </div> <div> <h4>IPSec Setup</h4> <div> <div>Phase 1 DH Group</div> <div>Phase 1 Encryption</div> <div>Phase 1 Authentication</div> <div>Phase 1 SA Life Time(s)</div> <div>Perfect Forward Secrecy</div> <div>Phase 2 DH Group</div> <div>Phase 2 Encryption</div> <div>Phase 2 Authentication</div> <div>Phase 2 SA Life Time(s)</div> <div>Preshared Key</div> <div>DPD Delay(s)</div> <div>DPD Timeout(s)</div> <div>DPD Action</div> </div> </div> </div>										

Image 4-50: VPN > Gateway to Gateway

#### Tunnel Name

Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created, each requiring a unique name.

Values (chars)

tunnel1

#### Enable

Used to enable (checked) is disable (unchecked) the VPN tunnel.

Values (checkbox)

Enable (Checked)



## 4.0 Configuration

### Local Group Setup

#### Gateway IP Address

Displays the IP address of the VIP4G, which is the local VPN Gateway.

Values (IP Address)

Current IP Address

#### Subnet IP Address

Define the local network by specifying the local subnet.

Values (IP Address)

#### Subnet Mask

Specify the subnet mask of the local network address.

Values (IP Address)

255.255.255.0

#### Group Server IP

In cases where a firewall is present, it may be required to specify the server IP. In cases where there is no firewall, usually this is the same as the Local Gateway IP Address.

Values (IP Address)

### Remote Group Setup

#### Gateway IP Address

Enter the IP address of the remote VPN Gateway.

Values (IP Address)

#### Server ID

In cases where a firewall is present, it may be required to specify the Server ID. In cases where there is no firewall, usually this is the same as the Remote Gateway IP Address.

Values (IP Address)

#### Subnet IP Address

Define the remote network by specifying the local subnet.

Values (IP Address)

#### Subnet Mask

Specify the subnet mask of the remote network address.

Values (IP Address)

255.255.255.0

## 4.0 Configuration

### IPsec Setup

#### Phase 1 DH Group

Select value to match the values required by the remote VPN router.

##### Values (selection)

**modp1024**  
modp1536  
modp2048

#### Phase 1 Encryption

Select value to match the Phase 1 Encryption type used by the remote VPN router.

##### Values (selection)

3des  
aes  
aes128  
aes256

#### Phase 1 Authentication

Select value to match the Phase 1 Authentication used by the remote VPN router.

##### Values (selection)

md5  
sha1

#### Phase 1 SA Life Time

Select value to match the values required by the remote VPN router.

##### Values

**28800**

#### Perfect Forward Secrecy (pfs)

Select value to match the values required by the remote VPN router.

##### Values (selection)

**Disable** / Enable

#### Phase 2 DH Group

Select value to match the values required by the remote VPN router.

##### Values (selection)

**modp1024**  
modp1536  
modp2048

#### Phase 2 Encryption

Select value to match the Phase 1 Encryption type used by the remote VPN router.

##### Values (selection)

3des  
aes  
aes128  
aes256

## 4.0 Configuration

### IPsec Setup

#### Phase 2 Authentication

Select value to match the Phase 1 Authentication used by the remote VPN router.

##### Values (selection)

md5  
sha1

#### Phase 2 SA Life Time

Select value to match the values required by the remote VPN router.

##### Values

3600

#### Preshared Key

Set the Preshared Key required to authenticate with the remote VPN router.

##### Values (characters)

password

#### DPD Delay(s)

Dead Peer Detection is used to detect if there is a dead peer. Set the DPD Delay (seconds), as required.

##### Values (seconds)

32

#### DPD Timeout(s)

Set the DPD (Dead Peer Detection) Timeout (seconds), as required.

##### Values (seconds)

122

#### DPD Action

Set the DPD action, hold or clear, as required.

##### Values (seconds)

Hold  
Clear

## 4.0 Configuration

### 4.9.3 VPN > Client To Gateway (L2TP Client)

The VIP4G can operate as a L2TP Client, allowing a VPN connection to be made with a L2TP Server.

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
<div>Summary Gateway To Gateway <b>Client To Gateway</b> VPN Client Access L2TP Server</div>										
<b>L2tp Client</b>										
<b>Add a New Tunnel</b>										
Tunnel Name <input type="text"/> Enable <input checked="" type="checkbox"/>										
<b>Local Group Setup</b>										
Gateway IP Address <input type="text" value="25.88.94.169"/>										
<b>Remote Group Setup</b>										
Gateway IP Address <input type="text"/>										
Server ID <input type="text"/>										
Group Subnet IP <input type="text"/>										
Group Subnet Mask <input type="text" value="255.255.255.0"/>										
<b>PPP Setup</b>										
Idle time before hanging up <input type="text" value="0"/> seconds [0...65535]										
PAP <input type="checkbox"/> Unencrypted Password										
CHAP <input checked="" type="checkbox"/> Challenge Handshake Authentication Protocol										
User Name <input type="text"/>										
Redial <input checked="" type="checkbox"/>										
Redial attempts <input type="text" value="3"/>										
Time between redial attempts <input type="text" value="15"/>										
<b>IPSec Setup</b>										
Preshared Key <input type="text"/>										
<input type="checkbox"/> Advanced+										

Image 4-51: VPN > Client to Gateway

#### Tunnel Name

Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created, each requiring a unique name.

Values (chars)

tunnel1

#### Enable

Used to enable (checked) is disable (unchecked) the VPN tunnel.

Values (checkbox)

Enable (Checked)

## 4.0 Configuration

### Local Gateway

The 4G IP Address is shown here and cannot be changed.

Values (IP Address)

*Current IP*

### Remote Gateway

Enter the IP Address of the Remote Gateway.

Values (IP Address)

*none*

### Remote Server ID

Enter the Remote Server ID as required by the L2TP server.

Values

*none*

### Remote Subnet IP

Enter the Remote Subnet IP.

Values (IP Address)

*none*

### Remote Subnet Mask

Enter the Remote Subnet Mask

Values (IP Address)

*none*

### Idle time before hanging up

Enter the Idle time (in seconds) to wait before giving up the PPP connection. The default is 0, which means the time is infinite. (0—65535)

Values (seconds)

*0*

### Username

Enter the Username

Values (chars)

*0*

### Preshared Key

The preshared key is required to connect to the L2TP Server.

Values (chars)

*0*

**IPSec Setup - See previous sections for additional info.**

## 4.0 Configuration

### 4.9.4 VPN > L2TP Server

System	Network	Carrier	Wireless	Comport	I/O	Firewall	Multicast	Qos	VPN	Tools
<div>Summary Gateway To Gateway Client To Gateway VPN Client Access <b>L2TP Server</b></div> <div> <b>L2tp Server</b> <div> Enable <input checked="" type="checkbox"/> </div> <div> <b>Server Setup</b> <div> Server IP Address <input type="text"/> IP Address Range Start <input type="text"/> IP Address Range End <input type="text"/> </div> </div> <div> <b>IPSec Setup</b> <div> Phase 1 DH Group <input type="text" value="modp1024"/> Phase 1 Encryption <input type="text" value="3des"/> Phase 1 Authentication <input type="text" value="md5"/> Phase 1 SA Life Time(s) <input type="text" value="28800"/> Perfect Forward Secrecy <input type="checkbox"/> Phase 2 DH Group <input type="text" value="modp1024"/> Phase 2 Encryption <input type="text" value="3des"/> Phase 2 Authentication <input type="text" value="md5"/> Phase 2 SA Life Time(s) <input type="text" value="3600"/> Preshared Key <input type="text"/> DPD Delay(s) <input type="text" value="32"/> DPD Timeout(s) <input type="text" value="122"/> DPD Action <input type="text" value="clear"/> </div> </div> </div>										

Image 4-52: VPN > L2TP Server

#### Enable

Used to enable (checked) is disable (unchecked) the L2TP Server.

Values (checkbox)

Enable (Checked)

#### Server IP Address

Enter the WAN or 4G IP address on which the L2TP server is to run.

Values (IP Address)

Current IP Address

#### IP Address Range Start - IP Address Range End

Define the range of IP addresses that can be assigned by the L2TP Server.

Values (IP Address)

**IPSec Setup - See previous sections for additional info.**



## 4.0 Configuration

### 4.9.5 VPN > VPN Client Access

For VPN L2TP Server operation, users will be required to provide a username and password. Use VPN Client Access to set up the required users.



microhard SYSTEMS INC.

System Network Carrier Wireless Comport I/O Firewall Multicast Qos **VPN** Tools

Summary Gateway To Gateway Client To Gateway **VPN Client Access** L2TP Server

**VPN Client Access**

Username

New Password

Confirm New Password

Image 4-53: VPN > VPN Client Access

#### Username

Enter a username for the user being set up.

Values (characters)

#### New Password

Enter a password for the use.

Values (characters)

#### Confirm New Password

Enter the password again, the VIP4G will ensure that the password match.

Values (IP Address)

## 4.0 Configuration

### 4.10 Tools

#### 4.10.1 Tools > Discovery

##### Network Discovery

The Network discovery tool allows the VIP4G to send a broadcast to all VIP4G/VIP Series units on the same network. Other units on the network will respond to the broadcast and report their MAC address, IP address (With a hyperlink to that unit's WebUI page), description, firmware version, operating mode, and the SSID (regardless of whether it was set to broadcast or not).

The discovery service can be a useful troubleshooting tool and can be used to quickly find and identify other units on the network. It can be disabled from the Network > sdpServer menu.



Image 4-54: Tools > Discovery

## 4.0 Configuration

### 4.10.2 Tools > Site Survey

#### Wireless Survey

The Wireless Survey feature will scan the available wireless channels for any other 802.11 wireless networks in proximity to the VIP4G. The Survey will display the Channel number the other networks are operating on, the MAC address, Encryption Type, Frequency and general signal level and quality information. This can be useful for finding available networks, or troubleshooting connection and sensitivity problems. If there are other networks operating on the same frequency, or a channel close to the one chosen, it can then be decided to try to use another channel.

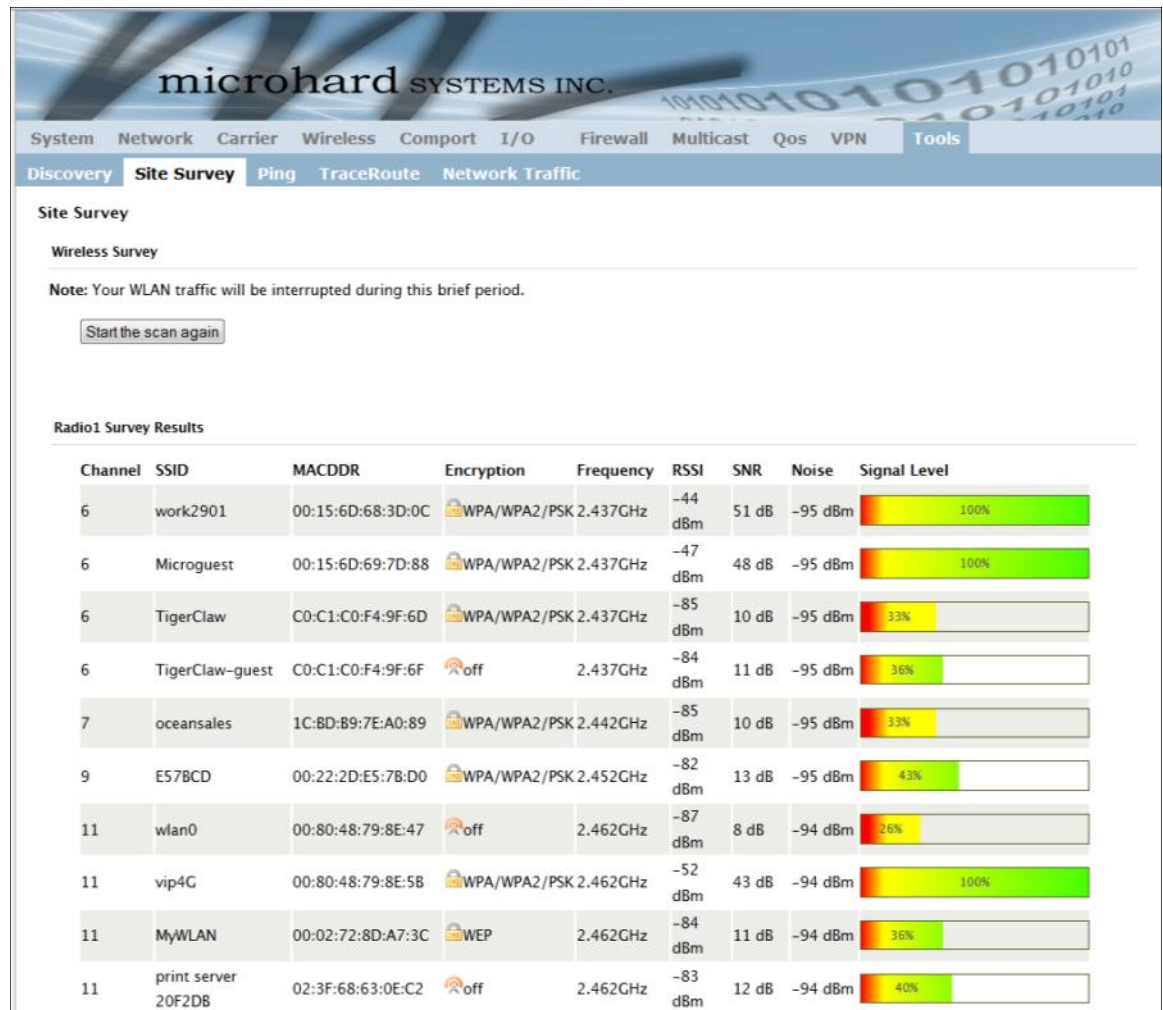


Image 4-55: Tools > Site Survey

## 4.0 Configuration

### 4.10.3 Tools > Ping

#### Network Tools Ping

The Network Tools Ping feature provides a tool to test network connectivity from within the VIP4G unit. A user can use the Ping command by entering the IP address or host name of a destination device in the Ping Host Name field, use Count for the number of ping messages to send, and the Packet Size to modify the size of the packets sent.

microhard SYSTEMS INC.

System Network Carrier Wireless Comport I/O Firewall Multicast Qos VPN Tools

Discovery Site Survey Ping TraceRoute Network Traffic

**Network Tools Ping**

Ping Network Utilities

Ping Host Name

Ping Count

Ping Size

Please wait for output of "ping -c 4 -s 56 google.com"... PING google.com (173.194.33.6): 56 data bytes

64 bytes from 173.194.33.6: seq=0 ttl=48 time=93.918 ms

64 bytes from 173.194.33.6: seq=1 ttl=48 time=73.339 ms

64 bytes from 173.194.33.6: seq=2 ttl=48 time=112.700 ms

64 bytes from 173.194.33.6: seq=3 ttl=48 time=72.355 ms

--- google.com ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 72.355/88.078/112.700 ms

Image 4-56: Tools > Ping

## 4.0 Configuration

### 4.10.4 Tools > TraceRoute

#### Network TraceRoute

The **Trace Route** command can be used to provide connectivity data by providing information about the number of hops, routers and the path taken to reach a particular destination.

microhard SYSTEMS INC.

System Network Carrier Wireless Comport I/O Firewall Multicast Qos VPN Tools

Discovery Site Survey Ping **TraceRoute** Network Traffic

**Network TraceRoute**

TraceRoute Network Utilities

Tracerout Host Name

Please wait for output "tracert google.com"...

tracert to google.com (173.194.33.7), 30 hops max, 38 byte packets

1 10.118.5.146 (10.118.5.146) 95.576 ms 61.777 ms 59.947 ms

2 10.118.5.145 (10.118.5.145) 47.849 ms 10.118.5.149 (10.118.5.149) 54.500 ms 57.354 ms

3 10.118.20.18 (10.118.20.18) 114.087 ms 10.118.20.22 (10.118.20.22) 87.384 ms 10.118.20.18 (10.118.20.18) 61.644 ms

4 10.118.20.93 (10.118.20.93) 48.004 ms 45.652 ms 49.766 ms

5 192.168.1.75 (192.168.1.75) 51.891 ms 66.177 ms 65.765 ms

6 192.168.1.18 (192.168.1.18) 47.757 ms 99.777 ms 59.980 ms

7 172.25.56.145 (172.25.56.145) 57.204 ms 59.400 ms 47.726 ms

8 10.118.4.97 (10.118.4.97) 92.030 ms 49.599 ms 59.843 ms

9 74.198.148.114 (74.198.148.114) 48.062 ms 49.400 ms 87.965 ms

10 24.153.3.97 (24.153.3.97) 53.992 ms 71.908 ms 66.810 ms

11 69.63.250.13 (69.63.250.13) 53.102 ms 81.992 ms 49.871 ms

12 pos-1-0-0.gw02.abcgy.phub.net.cable.rogers.com (24.153.4.77) 49.910 ms 55.343 ms 50.023 ms

13 69.63.248.254 (69.63.248.254) 62.068 ms 68.020 ms 60.128 ms

Image 4-57: Tools > TraceRoute



## 4.0 Configuration

### 4.10.5 Tools > Network Traffic

#### Network Traffic Monitor Tool

The Tools > Network Traffic tab displays a graphical display of all data Traffic on the VIP4G.

- br-lan** Shows an overview of all data sent or received by the VIP4G. A summary of the data of the current day and the current month is shown.
- br-lan / hourly** Shows the traffic volumes (TX = green, RX = grey) at hourly intervals during the current 24 hour period. This could be useful to see when the most or least amount of traffic is present.
- br-lan / daily** Shows the total data received and transmitted for the day, as well as the average rate of data.
- br-lan / monthly** Shows the total data received and transmitted for the current month, as well as the average rate of data.
- br-lan / Top 10** Show the top 10 days with the most data sent or received.

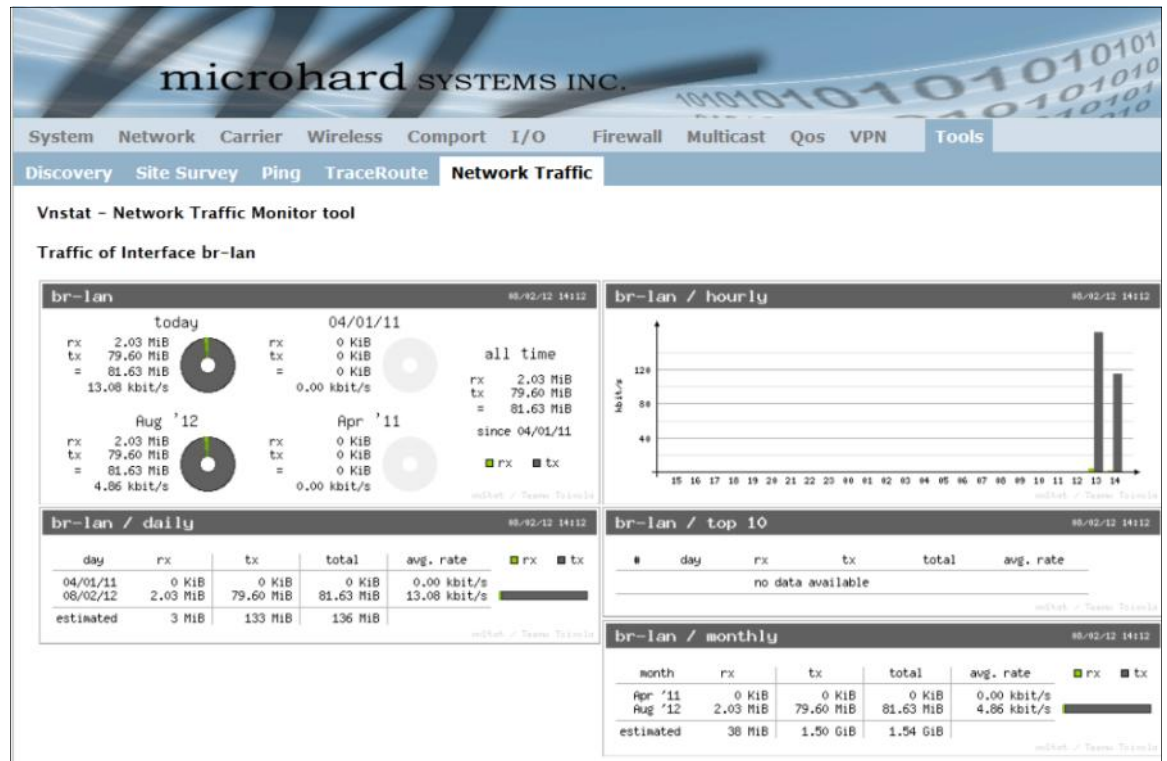


Image 4-58: Tools > Network Traffic



## Appendix A: Serial Interface

Module (DCE)	Signal	Host (e.g. PC) (DTE)	Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE, informing the DTE that a carrier is present).
1	DCD →	IN	The interface conforms to standard RS-232 signals, so direct connection to a host PC (for example) is accommodated.
2	RX →	IN	
3	← TX	OUT	
4	← DTR	OUT	
5	SG		
6	DSR →	IN	
7	← RTS	OUT	
8	CTS →	IN	The signals in the asynchronous serial interface are described below:

**DCD** *Data Carrier Detect* - Output from Module - When asserted (TTL low), DCD informs the DTE that a communications link has been established with another MHX 920A.

**RX** *Receive Data* - Output from Module - Signals transferred from the MHX 920A are received by the DTE via RX.

**TX** *Transmit Data* - Input to Module - Signals are transmitted from the DTE via TX to the MHX 920A.

**DTR** *Data Terminal Ready* - Input to Module - Asserted (TTL low) by the DTE to inform the module that it is alive and ready for communications.

**SG** *Signal Ground* - Provides a ground reference for all signals transmitted by both DTE and DCE.

**DSR** *Data Set Ready* - Output from Module - Asserted (TTL low) by the DCE to inform the DTE that it is alive and ready for communications. DSR is the module's equivalent of the DTR signal.

**RTS** *Request to Send* - Input to Module - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

**CTS** *Clear to Send* - Output from Module - A "handshaking" signal which is asserted by the DCE (TTL low) when it has enabled communications and transmission from the DTE can commence. When hardware handshaking is used, the CTS signal indicates to the host that the DCE can receive data.

Notes: It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

"DCE" and "module" are often synonymous since a module is typically a DCE device.

"DTE" is, in most applications, a device such as a host PC.

## Appendix C: Firmware Upgrade / Recovery

---

Package upgrade or recovery upgrade can be used. Package upgrade will keep settings intact. Recovery upgrade will upgrade a unit completely, it can also be used to recovery from a corrupted system.

Package upgrade (\*.pkg)

- Ø Download upgrade package and put it into a known directory;
- Ø Start up a command line window from the system;
- Ø Change current directory to where the package file is located;
- Ø Start a FTP session to the unit;
- Ø Provide proper user name and password to login; (username: upgrade; passwd: admin)
- Ø Change transfer protocol to \*BINARY\* mode;
- Ø Push package upgrade file into the system with “put” command;
- Ø Package upgrade takes up to 2 minutes to complete.

Recovery upgrade (\*.img)

- Ø Download recovery image and save it into a known directory;
- Ø Start up a command line window from the system;
- Ø Change current directory to where the package file is located;
- Ø Cycle power on the unit with CFG button pressed and held down until “RSSIs, TX and RX” LED is observed in flash mode;
- Ø Start a FTP session to IP address \*192.168.1.39 from LAN port\*;
- Ø Provide proper user name and password to login (username: upgrade; passwd: admin);
- Ø Change transfer protocol to \*BINARY\* mode;
- Ø Push package upgrade file into the system with “put” command;
- Ø Package upgrade takes more than 2 minutes to complete.
- Ø The unit automatically reboots after the recovery procedure is completed



150 Country Hills Landing NW  
Calgary, Alberta  
Canada T3K 5P3

Phone: (403) 248-0028  
Fax: (403) 248-2762  
[www.microhardcorp.com](http://www.microhardcorp.com)